

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局(43) 国際公開日  
2003 年 12 月 31 日 (31.12.2003)

PCT

(10) 国際公開番号  
WO 2004/001701 A1(51) 国際特許分類<sup>7</sup>:  
H03M 13/15, H04L 9/30, G06F 11/10

G09C 1/00,

中央研究所内 Tokyo (JP). 近藤 雄樹 (KONDOH, Yuki)  
[JP/JP]; 〒185-8601 東京都国分寺市東恋ヶ窪一丁目  
280番地 株式会社日立製作所 中央研究所内 Tokyo  
(JP).

(21) 国際出願番号: PCT/JP2002/006166

(22) 国際出願日: 2002 年 6 月 20 日 (20.06.2002)

(74) 代理人: 小川 勝男 (OGAWA, Katsuo); 〒103-0025 東京  
都中央区日本橋茅場町二丁目9番8号 友泉茅場町  
ビル 日東国際特許事務所 Tokyo (JP).

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(81) 指定国 (国内): CN, JP, KR, US.

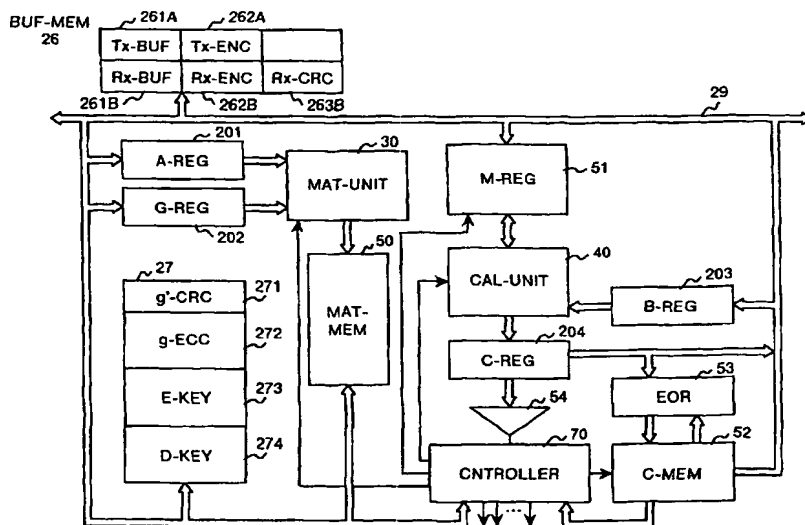
(71) 出願人 (米国を除く全ての指定国について): 株式会  
社日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010  
東京都千代田区神田駿河台四丁目6番地 Tokyo (JP).(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE,  
DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).添付公開書類:  
— 国際調査報告書

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 外村 元伸 (TONO-  
MURA, Motonobu) [JP/JP]; 〒185-8601 東京都国分寺  
市東恋ヶ窪一丁目280番地 株式会社日立製作所2文字コード及び他の略語については、定期発行される  
各PCTガゼットの巻頭に掲載されている「コードと略語  
のガイダンスノート」を参照。

(54) Title: CODE CALCULATING DEVICE

(54) 発明の名称: 符号演算装置



(57) Abstract: A product-sum calculating unit varies the parameters preset in first and second registers (201, 202) so as to instruct a matrix value calculating section (30) to calculate a matrix value for an error-detecting code (CRC) or for an elliptic curve cryptography (ECC). Then the unit changed the matrix value held in a matrix value register (51) so as to perform a product-sum calculation of the matrix value and data preset in a third register. Thus the unit is used commonly both for CRC encoding calculation and ECC encrypting calculation.

[続葉有]



---

(57) 要約:

第 1、第 2 レジスタ 201、202 に設定されたパラメータを変えることによって、誤り検出符号 (CRC) 用行列値又は楕円曲線暗号 (ECC) 用行列値を行列値演算部 30 で生成し、行列値レジスタ 51 に保持する行列値を切替えることによって、前記行列値と第 3 レジスタに設定されたデータとの積和演算を実行する積和演算部を CRC 符号化演算と ECC 暗号化演算とに共用する。

## 明 細 書

## 符号演算装置

## 技術分野

- 5 本発明は、通信データ用の符号演算装置に関し、更に詳しくは、デジタル・パケットデータの送受信において必要となる誤り検出(訂正)符号の生成とデータ暗号化／復号化処理のための符号演算装置に関する。

## 背景技術

- 10 デジタル通信装置では、データの機密性保持およびネットワーク上での信号誤りの発生に備えて、パケットデータの暗号化／復号化機能と誤り検出(訂正)符号の生成機能が必要となる。音声データやテキストデータの他に、情報量の多い静止画像や動画像等の通信ニーズが増えるに従って、デジタル通信装置には、データ転送速度の高速化に適した暗号化／復号化技術と誤り検出(訂正)符号の生成技術が要求されてきている。

- データパケットの誤り検出符号としては、例えば、誤り訂正は行わずに誤り検出のみを目的としたCRC (Cyclic Redundancy Check Codes: 巡回冗長検査符号) がよく使われる。CRC演算式については、例えば、Ramabadran, T.V. and Gaitonde S.S. "A Tutorial on CRC Computations", IEEE Micro, 20 vol. 8、 No. 4、 pp. 62-75、 Aug. 1988 に記載されている。

- 一方、データの機密性を保持するために使用される暗号方式としては、RSA暗号が有名である。しかしながら、RSAでは、暗号／復号鍵として1024ビットの長い符号を必要としているため、最近では、符号長が160ビット程度と短くて済む楕円曲線暗号 (ECC: Elliptic Curve Cryptography) が注目されている。楕円曲線暗号処理に関する文献としては、例えば、Moon, S.、 Park, J. and Lee, Y.、 "Fast VLSI Arithmetic Algorithms

for High-Security Elliptic Curve Cryptographic Applications”  
IEEE Trans. Consumer Electronics, vol.47, No.3, pp.700-708,  
Aug. 2001 がある。上記文献には、楕円曲線暗号 (E C C) に必要な演算  
式と、E C C 処理を実現した大規模集積回路の 1 例について説明され  
5 ている。

R S A は、桁上げ伝播が発生するモジュラー演算を採用しているため、ハードウェア量が多くなる。これに対して、E C C は、以下に説明するように、桁上げ伝播が発生しないガロア体 (有限体) をベースにしているため、データの暗号/復号化をコンパクトなハードウェアで実現できる。

- 10 式 (1) が示すガロア体上の  $n$  次多項式  $g(x)$  によるモジュラー演算 (mod) を考える。

$$g(x) = x^n + g_{n-1}x^{n-1} + \cdots + g_1x + 1 \quad (1)$$

- この多項式のガロア体は、一般に  $GF(2^n)$  と表記される。係数  $g_i$  の値は “0” または “1” であり、 $g_i \in GF(2)$  と表記される。また、  
15  $GF(2)$  の係数項内では、排他的論理和 (E O R) 演算 ( $\oplus$ ) が行われるが、本明細書では、特に混乱しない限り (+) 演算子で代用する。

今、長さ  $n$  のデータを表現する次の 3 つの多項式について考える。

$$a(x) = \sum_{i=0}^{n-1} a_i x^i, \quad b(x) = \sum_{i=0}^{n-1} b_i x^i, \quad c(x) = \sum_{i=0}^{n-1} c_i x^i,$$

但し、 $a_i, b_i, c_i \in GF(2)$

- 20 E C C の場合、共通鍵または秘密鍵と呼ばれる暗号鍵を示すデータを多項式  $a(x)$  とし、この暗号鍵が適用される送受信データを多項式  $b(x)$  とすると、送信側における暗号化データ、または受信側における復号化データ (元の平文データ) は、次式 (2) の演算結果  $c(x)$  として得られる。

25 
$$c(x) \equiv a(x) \cdot b(x) \bmod g(x) \quad (2)$$

式 (2) を詳しく書くと、次式 (3) になる。

$$\sum_{i=0}^{n-1} c_i x^i \equiv \left( \sum_{i=0}^{n-1} a_i x^i \right) \left( \sum_{i=0}^{n-1} b_i x^i \right) \mod g(x) \quad (3)$$

文献: Mastrovito, E. D., "VLSI Designs for Multiplication over Finite Fields  $GF(2^n)$ "、Proc. Sixth Int'l Conf. 「Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (AAECC-6)」 pp.297-309, Jul. 1988  
 5 と、公開公報 WO 91/20028 号（発明の名称「Universal Galois Field Multiplier」）において、Mastrovito は、式（3）を次の行列形式に変換することを試みている。

$$10 \quad \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} m_{00} & m_{01} & \cdots & m_{0,n-1} \\ m_{10} & m_{11} & \cdots & m_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n-1,0} & m_{n-1,1} & \cdots & m_{n-1,n-1} \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix} \quad (4)$$

$$c = M \cdot b \quad (5)$$

式（4）における  $n \times n$  の行列  $M$  は、Mastrovito 行列と呼ばれており、行列  $M$  の値は、多項式  $a(x)$  と  $g(x)$  から前もって計算することができる。

一方、CRC の値は、送信メッセージ（または受信メッセージ）の  
 15 データを多項式  $b(x)$  で示した場合に、次式（6）で示すように、 $x^n \cdot b(x)$  を多項式  $g(x)$  で割った時に得られる余り  $c(x)$  として算出される。

$$c(x) \equiv x^n \cdot b(x) \mod g(x) \quad (6)$$

ここで、 $x^n \cdot b(x)$  は、データ  $b(x)$  を  $n$  ビット左シフトすることを意味しており、データの送信側では、式（6）で算出された CRC の値：  
 20 多項式  $c(x)$  を送信データ  $b(x)$  に加算した形で、伝送路に送出する。

データの受信側では、CRC 付きの受信データ  $b(x)$  に対して同様の演算を行い、演算結果  $c(x)$  が 0 となった場合、極めて高い確率で受信

データ  $b(x)$  には誤りがないものと判定する。

式 (2) と式 (6) とを比較すると、CRC と ECC の演算式が極めて類似していることがわかる。両者の違いは、CRC の場合、データ  $b(x)$  に乗算される値が  $n$  次の  $x^n$  であるのに対して、ECC の場合は、  
5  $n-1$  次の多項式  $a(x)$  となっている点にある。

Mastrovito 行列について述べた上記文献では、BCH や Reed-Solomon と呼ばれる誤り訂正方式を式 (2) で一般的に取り扱おうとしているように思われる。しかしながら、上記文献には、これらの符号化方式を具体的にどのようにして式 (2) に結びつけるかについて具体的な記載がない。また、後  
10 述する本発明が着目した CRC 符号の行列表現に関して、上記文献には何ら示唆されていない。

#### 発明の開示

本発明の目的は、誤り検出処理と暗号／復号化処理に共用できる符号演算  
15 装置を提供することにある。

本発明の他の目的は、誤り検出処理と暗号／復号化処理に共用できるガロア体(有限体)符号演算装置を提供することにある。

本発明の更に他の目的は、誤り検出処理用と暗号／復号化処理用の行列値を同一の行列値演算部で算出し、これらの行列値を選択的に利用して、誤り  
20 検出処理と暗号／復号化処理を行うようにした符号演算装置を提供することにある。

本発明の更に他の目的は、コンパクトなハードウェア構成で誤り検出処理と暗号／復号化処理を実行できるパケット通信装置を提供することにある。

これらの目的を達成するために、本発明では、ガロア体ベースの CRC と  
25 ECC の演算式の類似性に着目し、CRC 演算と ECC 演算のためのハードウェアを共通化することを特徴とする。

CRCと楕円曲線暗号ECCの演算処理を共通化しようとした場合、容易に考えられる解決方法の1つは、式(2)で示したECC演算でデータ $b(x)$ に乘算される多項式 $a(x)$ の次数を $n-1$ 次から $n$ 次に上げることによって、式(6)で示したCRC演算における $x^n$ の次数と一致させておき、CRC演算を行う場合は、多項式 $a(x)$ の $n$ 次の係数部を使用する方法である。しかしながら、このように多項式 $a(x)$ の次数を増やす方法では、本質的な解決策とはならない。

本発明では、ガロア体モジュロ演算がもつ次の性質を利用して、CRCとECCの演算処理を共通化する。

すなわち、式(1)が示すように、ガロア体モジュロ演算に適用される既約多項式 $g(x)$ は、 $x^n$ の係数 $g_n$ が“1”となっている。そこで、式(6)が示すCRC演算に適用される $n$ 次以上の高次項 $x^n$ を $g(x)$ でモジュロ演算し、 $n-1$ 次以下の余りの項にリダクションすると、次の多項式(7)が得られる。

$$x^n \bmod g(x) \equiv g_{n-1}x^{n-1} + \dots + g_1x + 1 \quad (7)$$

ここで、式(7)の右辺を

$$g'(x) = g_{n-1}x^{n-1} + \dots + g_1x + 1 \quad (8)$$

と置き換えると、式(6)に示したCRCの演算式は、次式(9)のように変形され、ECCの演算式(2)と同様に、データ $b(x)$ に乘算される多項式の次数を $n-1$ 次にすることができる。

$$c(x) \equiv g'(x) \cdot b(x) \bmod g(x) \quad (9)$$

CRCの値は、 $a(x)$ に代えて $g'(x)$ の値をセットすることにより、式(9)に従って算出できる。

また、 $x^n$ よりも更に高次の項 $x^{n+1}$ を $g(x)$ でモジュロ演算すると、式(7)を利用して、次式(10)が示すように、 $n-1$ 次以下の項にリダクションできることが判る。

$$\begin{aligned}
 x^{n+1} \bmod g(x) &\equiv g_{n-1}x^n + g_{n-2}x^{n-1} + \dots + g_1x^2 + x \\
 &= g_{n-1}(g_{n-1}x^{n-1} + \dots + g_1x + 1) + g_{n-2}x^{n-1} + \dots + g_1x^2 + x \\
 &= (g_{n-1}g_{n-1} + g_{n-2})x^{n-1} + (g_{n-1}g_{n-2} + g_{n-3})x^{n-2} + \dots \\
 &\quad + (g_{n-1}g_2 + g_1)x^2 + (g_{n-1}g_1 + 1)x + g_{n-1} \quad (10)
 \end{aligned}$$

- 5 従って、 $n$  次以上の高次項は、 $n-1$  次以下の項にリダクションした後、 $x^i$  の係数項間を比較することによって、式 (4) または (5) の行列値を得ることができる。

- 本発明の特徴の 1 つは、CRC の演算式を式 (9) のように変形し、次数を ECC 演算式 (3) に適合させることによって、同一の行列値  
 10 演算部を利用して、ECC 用行列値と CRC 用行列値を計算できるようにしたことにある。また、本発明の他の特徴は、予め計算された ECC 用行列値と CRC 用行列値を選択的に利用することによって、同一の積和演算部で、ECC 符号化／復号化演算と CRC 演算を実行できるようにしたことにある。

15

#### 図面の簡単な説明

第 1 図は、本発明が適用される誤り検出機能と暗号処理機能を備えたパケット通信装置の構成を示すブロック図。

- 第 2 図は、CRC 誤り検出の符号化、復号化処理を説明するための  
 20 図。

第 3 図は、ECC 暗号化、復号化処理を説明するための図。

第 4 図は、行列演算回路 30 を備えた本発明による演算装置の 1 実施例を示すブロック図。

- 第 5 図は、行列演算回路 30 で生成される行列  $M$  の計算値配列を説  
 25 明するための図。

第 6 図は、 $n \times n$  の行列  $M$  の計算値を複数の部分行列に分割して生



成する場合の説明図。

第 7 図は、E C C 用の行列 M を構成する部分行列と入出力データとの関係を説明するための図。

第 8 図は、C R C と E C C に共用される行列値演算部 3 0 の 1 実施例を示す図。

第 9 図は、第 4 図に示したコントローラ 7 0 が実行する C R C 行列値生成ルーチン 1 0 0 の 1 実施例を示すフローチャート。

第 1 0 図は、コントローラ 7 0 が実行する E C C 用行列値生成ルーチン 1 2 0 の 1 実施例を示すフローチャート。

10 第 1 1 図は、コントローラ 7 0 が実行する送信データ処理ルーチン 2 0 0 と受信データ処理ルーチン 3 0 0 を示すフローチャート。

第 1 2 図は、送信データ処理ルーチン 2 0 0 における送信データ暗号化 2 1 0 の詳細を示すフローチャート。

15 第 1 3 図は、送信データ処理ルーチン 2 0 0 における C R C 生成 2 3 0 の詳細を示すフローチャート。

発明を実施するための最良の形態

第 1 図は、本発明が適用されるデータ誤り検出機能と暗号処理機能を備えたパケット通信装置のブロック図を示す。

20 パケット通信装置は、コアプロセッサ (P-CORE) 1 0 と、送受信データ処理部 2 0 と、伝送路 1 3 に接続された送信部 1 1 および受信部 1 2 とからなる。送信部 1 1 と受信部 1 2 は、伝送路 1 3 が無線の場合、A / D、D / A 変換器と、R F (Radio Frequency) 処理部とを含み、伝送路 1 3 がアナログ有線回線の場合は、モデム処理部を含む。

25 送受信データ処理部 2 0 は、制御プロセッサ (P-CONT) 2 1 と、暗号符号化部 (ECC-ENC) 2 2、誤り検出符号化部 (CRC-ENC) 2 3、誤り検出復号化部

(CRC-DEC) 24、暗号復号化部(ECC-DEC) 25と、バッファメモリ(BUF-MEM) 26、メモリ(MEM) 27からなり、これらの要素は、内部バス29(29A、29B)によって相互接続されている。

コアプロセッサ10から出力された送信メッセージ(平文データ)は、バッファメモリ26の送信バッファ領域に一時的に格納され、送信データに機密保持が必要な場合は、送信メッセージが暗号符号化部22で暗号化される。送信メッセージ(平文データまたは暗号化データ)は、誤り検出符号化部23で生成した誤り検出符号を付加した形で、送信部11から伝送路13に送出される。

- 10 逆に、伝送路13から受信した誤り検出符号付きの受信メッセージ(平文データまたは暗号化データ)は、受信部12からバッファメモリ26の受信バッファ領域に一旦格納され、誤り検出復号化部24で受信メッセージの誤り検出符号の余り演算が行われる。余りがゼロの場合、受信データに誤りがないものと判断し、受信メッセージから誤り検出符号が除去される。誤り検出符号を取り除いた受信メッセージのデータが暗号文の場合、暗号復号化部25で平文に戻した後、バッファメモリ26を介してコアプロセッサ10に転送される。誤り検出およびデータの暗号/復号化に必要な情報は、メモリ27から読み出され、暗号符号化部22、誤り検出符号化部23、誤り検出復号化部24、暗号復号化部25は、制御プロセッサ21に制御される。
- 20 第2図は、誤り検出にCRCを適用した場合の誤り検出符号化部23と誤り検出復号化部24の動作を示す。

- この場合、誤り検出符号化部23では、送信データを $n$ ビット長( $n = 32$ ビット)のデータブロック $b(x)$ に分割し、データブロック毎に符号化する。まず、式(6)が示すように、データ $b(x)$ を $n$ ビット左へシフト( $x^n \cdot b(x)$ の演算)した後、これを予め指定された数値 $g(x)$ で割って(モジュロ演算)、余り $r(x)$ を求める。
- 25

$$r(x) \equiv x^n \cdot b(x) \bmod g(x) \quad (11)$$

次に、 $r(x)$ をデータ  $x^n \cdot b(x)$ に加算、すなわち、 $w(x) = x^n \cdot b(x) \oplus r(x)$ の演算を行う。その結果、元の  $n$  ビットデータブロックは、 $2n$  ビット長のデータブロック  $w(x)$ に変換した形で伝送路に送出される。

- 5 一方、受信側の誤り検出復号化部24では、伝送路から受信したデータブロック  $w'(x) = x^n \cdot b'(x) \oplus r'(x)$ に対して、送信側と同一の数値  $g(x)$ でモジュロ演算を実行して、余りを求める。伝送路上で誤りが発生していなければ、次式(12)が成立し、余り  $c(x)$ がゼロになる。

$$c(x) \equiv [x^n \cdot b'(x) \oplus r'(x) \bmod g(x)]$$

$$10 \quad = r'(x) \oplus r'(x) \quad (12)$$

- この場合、受信データ  $w'(x)$ から  $r'(x)$ を除去し、 $n$  ビット右シフトすることによって、元のデータブロック  $b(x) = b'(x)$ を復元できる。尚、伝送路からの受信メッセージ長が  $2n$  ビットよりも長い場合は、 $2n$  ビット長のデータブロック毎に、上述した誤り検出復号化処理が繰り返される。
- 15

第3図は、暗号化にECCを適用した場合の暗号符号化部22と暗号復号化部25の動作を示す。

- 暗号符号化部22では、送信データを  $n$  ビットのデータブロックに分割し、送信データブロックを多項式  $b(x)$ 、共通鍵を多項式  $a(x)$ とし、既約多項式  $g(x)$ でモジュロ演算を実行することにより、式(2)が示す暗号化データ  $c(x)$ を生成する。
- 20

- ECC暗号符号化データのブロック長  $n$ は、CRCよりも長い160ビット程度になるため、CRCと同一ハードウェアを適用するために、送信データブロック  $b(x)$ 、共通鍵  $a(x)$ 、既約多項式  $g(x)$ をそれぞれCRCビット長に合わせた複数のサブブロック分割して、暗号化処理を繰り返す。
- 25

誤り検出符号が付加された暗号化データは、受信側で誤り検出され、もし、誤りがなければ、誤り検出符号を除去した暗号化データ  $c(x)$  に戻される。受信側の暗号復号化部 25 では、次式 (13) が示すように、式 (2) の  $a(x)$ 、 $b(x)$  の代わりに秘密鍵  $d(x)$  と受信データ  $c(x)$  を適用し、  
5 既約多項式  $g(x)$  によってモジュロ演算を実行することによって、復号化されたデータ  $b(x)$  を得る。

$$b(x) \equiv d(x) \cdot c(x) \bmod g(x) \quad (13)$$

本発明の特徴は、上述した誤り検出符号化部 23、誤り検出復号化部 24、暗号符号化部 22、暗号復号化部 25 に必要なハードウェアを共用することによって、送受信データ処理部 20 の構成を単純化したことにある。  
10

第 4 図は、本発明による送受信データ処理部 20 の 1 実施例を示す。

送受信データ処理部 (符号演算装置) 20 は、行列値演算部 (MAT-UNIT) 30、積和演算部 (CAL-UNIT) 40、制御部 (CONTROLLER) 70 と、バッファメモリ (BUF-NEM) 26、パラメータ格納用のメモリ 27、行列値格納用のメモリ (MAT-MEM) 50、行列値レジスタ (M-REG) 51、演算結果保持メモリ (C-MEM) 52 と、パラメータレジスタ (A-REG、G-REG) 201、202、データレジスタ (B-REG) 203、符号レジスタ (C-REG) 204 と、EOR 加算回路 53 と、一致検出回路 54 からなる。  
15

メモリ 27 は、CRC 演算で必要となるリダクションされた多項式  $g'(x)$  の記憶領域 ( $g'$ -CRC) 271 と、ECC 演算で必要となる既約多項式  $g(x)$  の記憶領域 ( $g$ -ECC) 272、暗号鍵 (公開鍵) の記憶領域 (E-KEY) 273 と、復号鍵 (秘密鍵) の記憶領域 (D-KEY) 274 とを含む。  
20

また、バッファメモリ 26 には、コアプロセッサ 10 から供給された送信メッセージの格納領域 (Tx-BUF) 261A、暗号化送信メッセージの格納領域 (Tx-ENC) 262A と、受信部から供給された CRC 付の受信メッセージの格納領域 (Rx-CRC) 263B、CRC 除去後の暗号化  
25

受信メッセージの格納領域(Rx-ENC) 2 6 2 B、復号化された受信メッセージの格納領域(Rx-BUF) 2 6 1 Bとが定義され、コアプロセッサ 1 0 と送受信データ処理部 2 0 との間では、Tx-BUF 領域 2 6 1 A と Rx-BUF 領域 2 6 1 B を介してメッセージが送受信される。

- 5      本実施例で示した送受信データ処理部(符号演算装置) 2 0 の動作モードには、行列値演算モードと、送信データ暗号化モードと、送信データ誤り符号化モードと、受信データ誤り検出モードと、暗号データ復号化モードとがある。これらの動作モードの切替えは、制御部 7 0 が行う。

- 10      行列値演算モードにおいて、例えば、ECC暗号化用の行列値を生成する場合は、制御部 7 0 が、メモリ領域 2 7 2 から読み出した既約多項式  $g(x)$  の値を G-REG 2 0 2 に設定し、メモリ領域 2 7 3 から読み出した暗号鍵を A-REG 2 0 1 に設定した状態で、行列値演算部 3 0 を起動する。生成された行列値は、メモリ 5 0 の暗号化用行列領域に保持される。

- 15      同様に、ECC復号化用の行列値は、メモリ領域 2 7 2 から G-REG 2 0 2 に既約多項式  $g(x)$  の値を設定し、メモリ領域 2 7 4 から A-REG 2 0 1 に復号鍵を設定した状態で生成され、行列値演算部 3 0 で生成された行列値は、メモリ 5 0 の復号用行列領域に保持される。

- 20      CRC用の行列値は、A-REG 2 0 1 と G-REG 2 0 2 にメモリ領域 2 7 1 から  $g'(x)$  の値を設定した状態で生成され、行列値演算部 3 0 で生成された行列値は、メモリ 5 0 のCRC用行列領域に保持される。

- 25      ここで、A-REG 2 0 1 と G-REG 2 0 2 を、例えば、CRC演算用のパラメータ長に合わせて 3 2 ビット長とした場合、CRC用の行列値は、これらのレジスタへの 1 回のパラメータロードで計算できる。しかしながら、ECC演算のパラメータは、CRC演算用のパラメータよりも長いため、ECC暗号化用および復号化用の行列値は、後述するように、メモリ 2 7 から既約多項式  $g(x)$  と暗号化鍵をそれぞれ 3 2 ビット単位で分割して読み出し、レジス

タ 2 0 1、2 0 2 の設定パラメータを切替えながら、行列値演算を複数回繰り返すことによって生成される。

送信データ暗号化モードでは、バッファメモリの Tx-BUF 領域から 3 2 ビットのサブブロック単位で読み出した送信データを B-REG 2 0 3 に  
5 供給し、送信データ暗号化に必要な部分行列値をメモリ 5 0 から M-REG 5 1 にロードして、積和演算部 4 0 を起動する。この場合、B-REG 2 0 3 に設定された 1 つのデータブロックに対して、M-REG 5 0 の内容を切替えながら、複数回の積和演算が繰り返される。

積和演算部 4 0 の演算結果は、C-REG レジスタ 2 0 4 に出力される。  
10 C-REG レジスタ 2 0 4 に出力された演算結果は、C-MEM 5 2 に中間演算値として保持される。C-MEM 5 2 は、E C C 符号長に応じたビット数の記憶容量を有し、積和演算サイクル毎に、EOR 加算回路 5 3 によって、新たな演算結果が部分行列と対応した中間演算値に加算される。

E C C 符号長に相当する複数サブブロック分の送信データについて  
15 暗号化演算処理が完了すると、C-MEM 5 2 の内容が暗号化データとして読み出され、バッファメモリ 2 6 の Tx-ENC 領域 2 6 2 A に転送される。

上述した積和演算の繰り返しによって、Tx-BUF 領域に格納された 1 メッセージ分の暗号化処理が完了すると、動作モードが送信データ誤り符号化モード（C R C 演算モード）に切り替えられる。

20 送信データ誤り符号化モードでは、MAT-MW0 5 0 から M-REG 5 1 に C R C 用の行列値をロードした状態で、バッファメモリ 2 6 の Tx-ENC 領域 2 6 2 A から、3 2 ビット単位で暗号化データブロックを読み出し、B-REG レジスタ 2 0 3 と送信部 1 1 に転送する。但し、送信データが暗号化を必要としない場合は、バッファメモリ 2 6 の Tx-BUF 領域 2 6 1  
25 A から読み出されたデータブロックが B-REG レジスタ 2 0 3 と送信部 1 1 に供給される。

積和演算部 40 は、B-REG レジスタ 203 のデータブロックと M-REG  
51 が示す CRC 用行列値との積和演算を実行し、演算結果を C-REG  
レジスタ 204 に出力する。この場合、C-REG レジスタ 204 に出力さ  
れた演算結果は、既に供給済みのデータブロックに付加すべき CRC  
5 符号として、バス 29 を介して送信部 10 に転送される。

受信データ誤り検出モードでは、バッファメモリ 26 の Rx-CRC 領域 26  
3B から読み出した受信データを対象として、積和演算部 40 により、  
B-REG レジスタ 203 のデータブロックと M-REG 51 の CRC 用行列  
値との積和演算を実行する。

10 この場合、Rx-CRC 領域 263B には、32 ビットのデータブロック毎に  
32 ビットの CRC 符号ブロックを付加した形で、受信データが格納されて  
いる。従って、受信データの誤りの有無は、例えば、第 1 サイクルで 32 ビ  
ットのデータブロックを読み出して  $CRC:r(x)$  を生成し、第 2 サイクルで、  
上記データブロックに続く 32 ビットの CRC 符号ブロックを読み出して C  
15  $R C:r'(x)$  を生成し、 $r'(x)$  と  $r(x)$  の一致を確認することによって判定  
できる。

上記  $r'(x)$  と  $r(x)$  との一致検出は、一致検出回路 54 で行われ、検出  
結果が制御部 70 に通知される。制御部 70 は、誤り検出を終えたデ  
ータブロックをバッファメモリの Rx-ENC 領域 262B (非暗号化デー  
20 タブロックの場合は Rx-BUF 領域 261B) に転送し、誤りのあるデー  
タブロックは廃棄する。

暗号データ復号化モードでは、Rx-ENC 領域 262B から読み出したデ  
ータブロックを対象として、積和演算部 40 で送信データ暗号化モー  
ドと同様の演算を行う。復号化されたデータは、C-MEM 52 から Rx-BUF  
25 領域 261B に転送される。

第 5 図は、行列値演算部 30 で生成される行列 M の 1 例を示す。

第4図の実施例では、行列値演算部30が $32 \times 32$ サイズの行列を生成するものとして説明したが、ここでは、簡単化のために、 $8 \times 8$ の行列を示す。 $b_0 \sim b_7$ は、B-REG 203に設定されるデータビット、 $c_0 \sim c_7$ は、演算結果としてC-REG 204に出力されるCRCまたはECCの  
5 ビットを示している。

行列Mの第1列の値( $m_{00} \sim m_{70}$ )は、多項式 $a(x)$ の各ビットの値( $a_0 \sim a_7$ )で決まる。

第2列以降の値( $m_{01} \sim m_{77}$ )は、基本的には

$$m(i, j) = m(i-1, j-1) + g(i) m(0, j) \quad (14)$$

10 の関係にあり、各列の第1行目の値( $m_{01}, m_{02}, m_{03} \dots m_{07}$ )は、

$$m(0, j) = g(0) m(\max, j-1) \quad (15)$$

の関係にある。ここで、 $m(\max, j-1)$ は、第 $j-1$ 列の最終行の行列値を意味している。

ここで、多項式 $g(x)$ の値は、規格で定められた固定値となる。また、  
15 ECC暗号化/復号化の場合、多項式 $a(x)$ は暗号鍵であり、或る期間内では固定の値(半固定値)となる。また、誤り検出の場合に、 $a(x)$ に代えて使用される多項式 $g'(x)$ は、完全な固定値である。従って、これらのパラメータから生成される行列Mは、固定または半固定値となるため、行列値演算部30で一度算出しておけば、演算結果を繰り返して  
20 利用できる。

行列演算部30と積和演算部40の行列演算能力は、ハードウェアの制約から、例えば、 $16 \times 16$ または $32 \times 32$ のように限られたサイズ(以下、基本サイズと言う)となる。基本サイズより大きい $n \times n$ サイズの行列Mを扱うためには、行列Mを基本サイズをもつ複数  
25 の部分行列に分割し、部分行列毎の演算動作を繰り返す必要がある。

第6図は、 $n \times n$ の行列Mを部分行列 $M(0, 0) \sim M(I, J)$ に分割した



例を示す。

ここで、例えば、最初の部分行列 $M(0, 0)$ における第2列（データビット $b_1$ 列）の第1行（演算結果 $c_0$ の行）の行列値 $m(0, 1)$ は、行列 $M$ の左下に位置した部分行列 $M(I, 0)$ における第1列（データビット $b_0$ の列）の最終行の行列値 $m(n-1, 0)$ に依存している。図面では省略されている次の部分行列 $M(1, 0)$ における第2列第1行の行列値 $m(k, 1)$ は、上記最初の部分行列 $M(0, 0)$ における第1列最終行の行列値 $m(k-1, 0)$ に依存している。また、行列 $M$ 全体における第1列（データビット $b_0$ の列）を除いて、各列では、行列 $M$ の第1行目（演算結果 $c_0$ の行）の値が後続する全ての行（演算結果 $c_1 \sim c_{n-1}$ の行）に反映されている。

従って、行列演算部30で部分行列毎に行列値を生成する場合は、これらの境界条件を考慮したパラメータ設定が必要となる。

第7図は、 $160 \times 160$ ビットの行列を $32 \times 32$ の基本サイズをもつ複数ブロックに分割した場合の部分行列 $M(0, 0) \sim M(4, 4)$ の配列と、入力データ（B01～B159）、出力符号（C01～C159）の関係を示す。

このような部分行列を扱う場合、積和演算部40には、入力データ（B01～B159）が32ビット単位のデータブロックD-0～D-4分割した形で入力され、出力符号（C01～C159）が32ビット単位の符号ブロックECC-0～ECC-4に分割した形で出力されることになる。

第8図は、ECC行列値を $32 \times 32$ ビットの部分行列毎に生成するようにした行列値演算部30の1実施例を示す。

行列値演算部30は、A-REG 201およびG-REG 202の各ビットと対応して用意された複数のAND回路 $31-i$ 、第1のセクタ群 $33-i$ および排他論理和（EOR）回路 $32-i$ （ $i=0 \sim k$ 、 $k=31$ ）と、これらのEOR回路の出力値を保持するための複数ビットの記憶領域 $35-i$ （ $i=0 \sim k$ ）をもつレジスタ35とからなる。

- EOR 回路 32-i の第1入力には、制御部 70 からの制御信号 S0 で制御されるセクタ 33-i を介して、A-REG 201 の第 i ビットの値  $a_i$  と AND 回路 31-i の出力値の何れかが選択的に供給される。最初の EOR 回路 32-0 を除いて、EOR 回路 32-i ( $i = 1 \sim k$ ) に
- 5 は、レジスタ 35 に保持された前列前行の行列値  $m(i-1, j-1)$  が第2入力として供給される。最初の EOR 回路 32-0 の第2入力には、制御部 70 からの制御信号 S2 で制御されるセクタ 37 を介して、固定値 “0” またはレジスタ 35 の最終ビット記憶領域 35-k に保持された前列最終行の行列値  $m(31, j-1)$  が供給される。
- 10 セクタ 33-0 から出力される部分行列第1行目の行列値は、制御部 70 からの制御信号 S3 で指定される所定のタイミングで、ラッチ回路 34 に保持される。
- AND 回路 31-i には、G-REG 202 の第 i ビットの値  $g_i$  が第1入力として供給される。最初の AND 回路 31-0 の第2入力には、
- 15 セクタ 36-0 を介して、前列最終行の行列値  $m(31, j-1)$  と上記ラッチ回路 34 に保持された部分行列第1行目の行列値の何れかが供給される。他の AND 回路 31-i ( $i = 1 \sim k$ ) の第2入力には、セクタ 36-i を介して、セクタ 33-0 の出力値またはラッチ回路 34 に保持された部分行列第1行目の行列値の何れかが供給される。
- 20 セクタ 36-0 ~ 36-k は第2のセクタ群を構成しており、制御部 70 からの制御信号 S1 で制御される。
- 本実施例では、CRC 用行列演算と ECC 用行列演算に共用するために、行列値演算部 30 が、EOR 回路 32-i の出力ビットを保持するためのシフトレジスタ (SHIFT) 38-i と、シフトレジスタ 38-i の
- 25 出力値とレジスタ領域 35-i の出力値の何れかを選択して次行 EOR 回路 32-(i+1) に供給する第3のセクタ群 39-i ( $i = 0 \sim$

k)を備えている。第3のセクタ群は、制御信号S1で制御される最後のセクタ $39-k$ を除いて、制御信号S4に応じてAポート、Bポートの何れかの入力を選択する。

CRC用の行列値を生成する場合、制御部70は、セクタ37と  
 5 第2セクタ群 $36-0 \sim 36-k$ と第3のセクタ群 $38-0 \sim 38-k$ が常時Aポート入力を選択するように、制御信号S1、S2、S4を出力する。また、第1セクタ群 $33-0 \sim 33-k$ が、行列Mの第1列目の行列値演算サイクルではAポート入力(A-REG出力)、第2列  
 10 D回路 $31-i$ の出力)を選択するように、制御信号S0が切替えられる。

従って、第1列目の行列値演算サイクルでは、EOR回路 $32-i$  ( $i=0 \sim k$ )から、A-REG 201が示す各ビットの値 $a_0 \sim a_{31}$ が生成される。これらのビット値は、レジスタ35の各記憶領域 $35-0 \sim 35-k$ に設定された後、MAT-MEM 50のCRC用行列領域、図示した例  
 15 ではM(0,0)の第1列目に記憶される。

次の、第2列目の行列値演算サイクルでは、第1行目のセクタ $33-0$ から、セクタ $36-0$ で選択された記憶領域 $35-k$ が示す前サイクル最終行の行列値 $a_{31}$ とG-REG 202が示す第1ビットの値  
 20  $g_0$ との間の論理積を示す値( $m_{0,1}$ )が出力され、EOR回路 $32-0$ に入力される。上記値 $m_{0,1}$ は、第2のセクタ群 $36-i$  ( $i=1 \sim k$ )を介して他のAND回路 $31-i$ にも入力される。従って、第1行目以降のセクタ $33-i$ からは「 $g_i \cdot m_{0,1}$ 」を示す値が出力され、EOR回路 $32-i$ から式(14)が示す行列値が出力される。

25 第2列目～第k列目の各演算サイクルで、上記と同様の演算動作を繰り返すことによって、CRC用行列領域M(0,0)に式(14)、(1

5) に従った行列値を生成することができる。

一方、ECC用の行列値を生成する場合は、第3のレジスタ群  $39-i$  ( $i=0\sim k$ ) にBポート入力を選択させた状態で、A-REG 201の設定パラメータを入れ替えながら、行列Mの第1列目の行列値演算  
5 サイクルが繰り返される。これらの演算サイクルで、レジスタ35に  $a_0\sim a_{31}$ 、 $a_{32}\sim a_{63}$ 、 $\dots a_{128}\sim a_{159}$  の値が次々と生成され、部分行列M  $(0,0)$ 、 $M(1,0)$ 、 $\dots M(4,0)$  の第1列目に記憶される。

この時、最初のシフトレジスタ  $38-0$  には、 $a_0$ 、 $a_{32}$ 、 $a_{64}$ 、 $a_{96}$ 、 $a_{128}$  のビット値が保持され、次のシフトレジスタ  $38-1$  に  
10 は、 $a_1$ 、 $a_{33}$ 、 $a_{65}$ 、 $a_{97}$ 、 $a_{129}$  のビット値、最後のシフトレジスタ  $38-k$  には、 $a_{31}$ 、 $a_{63}$ 、 $a_{92}$ 、 $a_{127}$ 、 $a_{159}$  のビット値が保持された状態となる。

第1列目の行列値演算が終了すると、制御信号  $S_0$  と制御信号  $S_2$  によって、第1セクタ群  $33-i$  とセクタ37がそれぞれのBポート  
15 入力を選択するように切替える。この時点では、レジスタ35の記憶領域  $35-k$  には、行列値  $m_{31,j-1}$  としてパラメータ値 " $a_{159}$ " が設定されている。

以下、G-REG 202の設定値を入れ替えながら、部分行列M  $(0,0)$ 、 $M(1,0)$ 、 $\dots M(4,0)$  の第1列目の行列値演算サイクルを繰り返す。

20 G-REG 202に第1ブロックのパラメータ値  $g_0\sim g_{31}$  を設定した演算サイクルでは、制御信号  $S_1$  の切替えによって、第2セクタ群  $36-i$  と、第2セクタ群の最後のセクタ  $39-k$  にAポート入力を選択させ、セクタ  $33-0$  の出力値 " $g_0 \cdot a_{159}$ " を他の行のAND回路  $31-i$  に入力する。また、制御信号  $S_3$  で与えるラッチ  
25 指令によって、上記セクタ  $33-0$  の出力値 " $g_0 \cdot a_{159}$ " をラッチ回路34に記憶する。この時、EOR回路  $32-j$  には、シフトレジス

タ 38-(j-1)から出力された前列前行のビット値 $m(0, j-1)$ が入力されるため、式(14)、(15)に従った第2行目の行列値 $m_{0,1} \sim m_{31,1}$ が生成され、これらの値が、シフトレジスタ38-0~38-kとMAT-MEM50のECC用部分行列 $M(0,0)$ の第2列目に記憶される。

- 5 G-REG 202に第1ブロック( $g_{32} \sim g_{63}$ )~第4ブロック( $g_{127} \sim g_{159}$ )のパラメータ値を設定した状態で行われる各演算サイクルでは、制御信号S1との切替えによって、第2セクタ群36-iと、第3セクタ群の最後のセクタ38-kにBポート入力を選択させる。すなわち、部分行列 $M(1,0) \sim M(4,0)$ の行列値に、上記ラッ
- 10 チ回路34に記憶された“ $g_0 \cdot a_{159}$ ”を反映させる。これによって、式(14)、(15)に従った第1行目の行列値( $m_{32,1} \sim m_{63,1}$ )~( $m_{127,1} \sim m_{159,1}$ )が次々と生成され、MAT-MEM50の部分行列 $M(1,0) \sim M(4,0)$ の第2列目に記憶される。

- 部分行列 $M(0,0)$ 、 $M(1,0)$ 、 $\dots M(4,0)$ の第3列目~第32列
- 15 目の行列値は、上述した第2列目と同様の手順を繰り返すことによって生成でされる。残りの部分行列 $M(0,1)$ 、 $M(1,1)$ 、 $\dots M(4,4)$ では、第1列から第32列までの全ての行列値演算にG-REG202の設定値を利用し、部分行列 $M(0,0)$ 、 $M(1,0)$ 、 $\dots M(4,0)$ の第2列目以降の演算サイクルと同様の手順を繰り返す。

- 20 第9図は、第8図に示した行列値演算部30を制御対象として制御部70が実行するCRC行列値生成ルーチン100の1実施例を示す。

- CRC行列値生成ルーチン100では、列を指定するためのパラメータiを初期値0、最後の列を示すパラメータjmaxの値を「31」に設定(ステップ101)した後、メモリ領域271から読み出した
- 25  $g'$ -CRCの値をA-REG201とG-REG202にロードする(ステップ102、103)。次に、制御信号S1~S4の発生パターンを単一行列モ

ードに設定する。ここで、単一行列モードは、行列値の演算が基本サイズ  $32 \times 32$  ビットの単一の部分行列で完了することを意味しており、このモードでは、制御信号 S1、S2、S4 は、第 2、第 3 のセクタ群  $36-i$ 、 $39-i$  ( $i=0 \sim k$ ) とセクタ 37 に常時 A ポート  
5 入力を選択させた状態となり、制御信号 S3 は、ラッチ信号を全く発生しない状態となる。

先ず、制御信号 S0 によって、第 1 セクタ群  $33-i$  ( $i=0 \sim k$ ) に A-REG 201 の出力 (A ポート入力) を選択させ (105)、EOR 回路  $32-i$  ( $i=0 \sim k$ ) により第  $j$  列の行列値を演算する (10  
10 6)。EOR 回路から出力された第  $j$  列の演算結果は、レジスタ 35 に保持した後、MAT-MEM 50 に定義された CRC 用の行列領域に記憶する (107)。制御信号 S0 の状態を切替えて、第 1 セクタ群 33 に G-REG 202 の出力 (B ポート入力) を選択させる (108)。

次に、パラメータ  $j$  の値をインクリメントし (109)、 $j$  の値を  
15  $j_{\max}$  と比較する (110)。  $j > j_{\max}$  となっていた場合は、このルーチンを終了し、そうでなければ、パラメータ  $j$  が示す次列の行列値を EOR 回路  $32-i$  により演算し (111)、第  $j$  列の演算結果を CRC 用の行列領域に記憶する (112)。この後、ステップ 109 に戻り、 $j > j_{\max}$  となる迄、同様の動作を繰り返す。

20 CRC 用の行列 M のサイズは、行列値演算部 30 が扱う基本サイズとなっているため、上述したように、 $j=0 \sim j_{\max}$  の行列値の演算を繰り返すことによって、積和演算部 40 が必要とする全ての行列値を生成できる。

第 10 図は、第 8 図に示した行列値演算部 30 を制御対象として制  
25 御部 70 が実行する ECC 行列値生成ルーチン 120 の 1 実施例を示す。

E C C 行列値生成ルーチン 1 2 0 では、図 7 に示した部分行列 M (I, J) を特定するためのパラメータ I、J の値と、部分行列 M (I, J) 内での列番号を指定するためのパラメータ j の値を初期値 0 に設定し、パラメータ I と J の最大値 I<sub>max</sub> と J<sub>max</sub> を 4、j の最大値 j<sub>max</sub> を 3 1  
5 に設定する (1 2 1)。

次に、制御信号 S1、S2、S3、S4 の発生パターンを部分行列モードに設定する。ここで、部分行列モードは、行列値の演算が複数の部分行列に分割して実行されることを意味しており、このモードでは、制御信号 S1 は、第 2 セレクタ群 3 6 - i (i = 0 ~ k) とセレクタ 3 9 -  
10 k が、部分行列 M (0, J) の演算サイクルでは A ポート入力、その他の部分行列 M (I, J) (但し、I = 1 ~ 4) の演算サイクルでは B ポート入力を選択するように切替えられ、制御信号 S2 は、セレクタ 3 7 が、部分行列 M (I, 0) (但し、I = 0 ~ 4) の第 1 列の演算サイクルでは A ポート入力、その後は B ポート入力を選択するように切替えられる。

15 また、制御信号 S3 は、部分行列 M (0, J) の各列の演算サイクルでラッチ信号を発生し、ラッチ回路 3 4 にセレクタ 3 3 - 0 の出力値を保持させる。ラッチ回路 3 4 の出力値は、部分行列 M (1, J) ~ M (4, J) の演算サイクルでは不変となる。制御信号 S4 は、第 3 セレクタ群 3 9 - i (i = 0 ~ k - 1) に常時、A ポート入力を選択させる。

20 先ず、制御信号 S0 によって、第 1 セレクタ群 3 3 - i (i = 0 ~ k) に A-REG 2 0 1 の出力 (A ポート入力) を選択させ (1 2 3)、メモリ 2 7 の E-KEY 領域 2 7 3 から A-REG 2 0 1 に暗号鍵の第 I ブロック KEY(I) をロードする (1 2 4)。この時、EOR 回路 3 2 - i (i = 0 ~ k) は、KEY(I) が示す 3 2 ビットのパラメータに従って、部分行列 M  
25 (I, J) の第 1 列の行列値を演算する (1 2 5)。この演算結果は、シフトレジスタ 3 8 とレジスタ 3 5 に保持した後、MAT-MEM 5 0 に定義され

た ECC 用部分行列領域  $M(I, J)$  の第  $j$  列に記憶される (1 2 6)。

次に、パラメータ  $I$  の値をインクリメントし (1 2 7)、 $I$  の値を  $I_{\max}$  と比較する (1 2 8)。 $I > I_{\max}$  でなければ、ステップ 1 2 4 に戻って、E-KEY 領域 2 7 3 から暗号鍵の次のブロック  $KEY(I)$  を A-REG 5 2 0 1 にロードし、同様の動作を繰り返す。

$I > I_{\max}$  となった場合は、制御信号  $S0$  の状態を切替えて、第 1 セレクタ群 3 3 に G-REG 2 0 2 の出力 (B ポート入力) を選択させ (1 3 0)、パラメータ  $I$  を初期値 0 に戻し、パラメータ  $j$  の値をインクリメントする (1 3 3)。

10 次に、パラメータ  $j$  の値を  $j_{\max}$  と比較し (1 3 4)、 $j > j_{\max}$  でなければ、メモリ 2 7 の  $g$ -ECC 領域 2 7 2 から A-REG 2 0 1 に多項式  $g(x)$  の第  $I$  ブロック  $g$ -ECC( $I$ ) をロードする (1 3 5)。これによって、EOR 回路 3 2 -  $i$  ( $i = 0 \sim k$ ) で、 $g$ -ECC( $I$ ) が示す 3 2 ビットのパラメータに従った部分行列  $M(I, J)$  の第  $j$  列の行列値が演算される (1 3 6)。演算結果は、レジスタ 3 5 に保持した後、MAT-MEM 5 0 に定義された ECC 用部分行列領域  $M(I, J)$  の第  $j$  列に記憶される (1 3 7)。

次に、パラメータ  $I$  の値をインクリメントし (1 3 8)、 $I$  の値を  $I_{\max}$  と比較する (1 3 9)。 $I > I_{\max}$  でなければ、ステップ 1 3 5 に戻って、E-KEY 領域 2 7 3 から  $g(x)$  の次のブロック  $g$ -ECC( $I$ ) を A-REG 20 2 0 1 にロードし、同様の動作を繰り返す。ステップ 1 3 9 で  $I > I_{\max}$  となった場合は、ステップ 1 3 3 に戻り、パラメータ  $I$  を初期値 0 に戻し、パラメータ  $j$  の値をインクリメントして、次列の行列値について上記と同様の手順を繰り返す。

ステップ 1 3 4 で  $j > j_{\max}$  となった場合、ステップ 1 4 0 に進み、25 パラメータ  $j$  と  $I$  の値を初期値 0 に戻し、パラメータ  $J$  の値をインクリメントする。これによって、次列の部分行列  $M(I, J)$  が演算対象とな



る。パラメータ  $J$  の値を  $J_{\max}$  と比較し (1 4 1)、 $J > J_{\max}$  となっていた場合は、このルーチンを終了する。 $J > J_{\max}$  でなければ、ステップ 1 3 5 に進む。これによって、部分行列  $M(0, J) \sim M(4, J)$  内の第 1 列から第 3 2 列について、上述した行列値の演算動作が繰り返される。

- 5 尚、上記ステップ 1 3 3 ~ 1 4 1 の実行過程で、部分行列  $M(0, J)$  の各列の演算サイクルで、制御信号  $S3$  で与えるラッチ指令によって、行列  $M$  の第 1 行目の行列値がラッチ回路 3 4 に保持され、この値が後続する部分行列  $M(1, J) \sim M(4, J)$  の各演算サイクルで AND 回路 3 1 - 0 ~ 3 1 -  $k$  に供給される。また、第 8 図に示した第 1 行の EOR 回路
- 10 3 2 - 0 には、レジスタ 3 5 の最後の記憶領域 3 5 -  $k$  から出力される前列最終行の行列値が供給されているため、第 6 図で説明した部分行列間の境界条件を満たすことができる。

- 以上、ECC 暗号化用の行列値生成ルーチンについて説明したが、ブロック KEY(I) として、メモリ 2 7 の D-KEY 領域から読み出した復号
- 15 鍵を適用すれば、ルーチン 1 2 0 と同様の制御手順で ECC 復号化用の行列値を生成できる。

第 1 1 図の (A) と (B) は、積和演算部 4 0 を制御対象として制御部 7 0 が実行する送信データ処理ルーチン 2 0 0 と受信データ処理ルーチン 3 0 0 のフローチャートを示す。

- 20 送信データ処理ルーチン 2 0 0 は、バッファメモリ 2 6 の Tx-BUF 領域 2 6 1 A から読み出した送信データ (送信メッセージ) の暗号化処理 (2 1 0) と、Tx-ENC 領域 2 6 2 A から読み出した暗号化データについての CRC 生成/送信処理 (2 3 0) とからなる。但し、送信データの暗号化が不要の場合は、Tx-BUF 領域 2 6 1 A から読み出した送
- 25 信データを処理対象として、CRC 生成/送信処理 (2 3 0) が実行される。

一方、受信データ処理ルーチン 300 は、バッファメモリ 26 の Rx-CRC 領域 263 B に蓄積された受信データについての CRC 生成処理 (310) と、CRC チェック (320) の結果、誤りなしと判定された受信データを対象とした復号化処理 (330) とからなる。復  
5 号化処理 (330) では、受信データが暗号化データか否かを判定し、暗号化データでなければ、受信データをそのまま Rx-BUF 領域 161 B に転送し、暗号化データの場合には、これを復号化した後、Rx-BUF 領域 161 B に転送する。CRC チェックの結果、誤りが検出された受信データについては、例えば、上位装置であるコアプロセッサ 10 へ  
10 のエラー通知などのエラー処理 (350) が実行される。

上記送信データ処理ルーチン 200 と受信データ処理ルーチン 300 は、メッセージ単位で交互に実行される。

第 12 図は、送信データの暗号化処理 210 の 1 実施例を示すフローチャートである。

15 制御部 70 は、Tx-BUF 領域 261 A から送信メッセージのヘッダ部を読み出し (211)、ヘッダ部が示すデータ長 L から、送信データを暗号化データのブロック長、この例では 160 ビット単位で分割した場合のブロック数  $N_{max}$  を計算し、暗号化処理の繰り返し回数を示すパラメータ  $n$  の値を初期値 1 に設定する (212)。本実施例では、  
20 ヘッダ部は暗号化の対象外とし、Tx-ENC 領域 262 A に転送する (213)。

先ず、部分行列  $M(I, J)$  を指定するためのパラメータ  $I$ 、 $J$  の値を初期値 0 に設定し (214)、Tx-BUF 領域 261 A から、送信データの  $n$  番目のデータブロックを 32 ビット単位で読み出し、B-REG 203 に  
25 転送する (215)。ここでは、B-REG 203 に読み出された 32 ビットのデータブロックを  $D(n)-J$  で表す。最初に読み出されたデータプロ

ック  $D(n)-0$  は、第 7 図におけるデータ  $D-0$  に相当し、その次に読み出されるデータブロック  $D(n)-1$  は、データ  $D-1$  に相当する。

次に、メモリ 5 0 から M-REG 5 1 に暗号化用の部分行列  $M(I, J)$  をロード (2 1 6) し、積和演算部 4 0 を起動すると (2 1 7)、C-REG 5 2 0 4 に部分行列  $M(I, J)$  とデータ  $D(n)-J$  との積和演算結果が出力される。部分行列  $M(0, 0)$  を使用した最初の積和演算では、第 7 図に示した  $C0 \sim C31$  の値が求まる。この値は、ECC 符号の部分計算値に過ぎないため、C-MEM 5 2 の ECC-I 領域の既演算値に EOR 加算する (2 1 8)。C-MEM 5 2 には、部分行列  $M(I, J)$  のパラメータ  $J$  と対応して、  
10 3 2 ビット長の符号値記憶領域 ECC-0  $\sim$  ECC-4 が用意しており、各領域の初期値は 0 となっている。

パラメータ  $I$  の値をインクリメントし (2 1 9)、 $I > 4$  か否かを判定する (2 2 0)。  $I$  の値が 4 以下であれば、ステップ 2 1 6 に戻り、上述した動作を繰り返す。これによって、データ  $D-0$  と部分行列  
15  $M(1, 0) \sim M(4, 0)$  の積和演算が次々と実行され、演算結果  $C32 \sim C63 \sim C128 \sim C159$  が C-MEM 5 2 の ECC-1  $\sim$  ECC-4 の既演算値に EOR 加算される。

パラメータ  $I$  をインクリメントした結果、 $I > 4$  となった場合は、 $I$  の値を初期値 0 に戻し、 $J$  の値をインクリメントして (2 2 1)、  
20  $J > 4$  か否かを判定する (2 2 2)。  $J$  の値が 4 以下の場合は、ステップ 2 1 5 に戻って、Tx-BUF 領域 2 6 1 A から B-REG 2 0 3 に、送信データの次のブロック  $D(n)-J$  を転送し、ステップ 2 1 5  $\sim$  2 2 2 の動作を繰り返す。  $J$  の値が 4 を超えるまで、上述した動作を繰り返すことによって、第 7 図に示したデータ  $D-1$  と部分行列  $M(0, 1) \sim M(4, 1)$ 、  
25 データ  $D-2$  と部分行列  $M(0, 2) \sim M(4, 2)$ 、データ  $D-3$  と部分行列  $M(0, 3) \sim M(4, 3)$ 、データ  $D-4$  と部分行列  $M(0, 4) \sim M(4, 4)$  の積和演算が次々と

実行され、各積和演算の結果が C-MEM 5 2 の ECC-0~ECC-4 に次々と EOR 加算される。

パラメータ J の値が  $J > 4$  となった時、C-MEM 5 2 の内容 (ECC-0~ECC-4) は、1 6 0 ビット長送信データについての暗号化結果を示している。従って、C-MEM 5 2 の内容をバッファメモリの Tx-ENC 領域 2 6 2 A に転送し (2 2 3)、C-MEM 5 2 の ECC-0~ECC-4 をクリア (2 2 4) した後、パラメータ n の値をインクリメントする (2 2 5)。n の値を最大値 Nmax と比較し (2 2 6)、 $n > Nmax$  でなければ、ステップ 2 1 4 に戻って、次の 1 6 0 ビット長の送信データ D(n) を対象として、暗号化処理を繰り返す。n > Nmax となった時点で、1 つの送信メッセージの暗号化が完了する。

第 1 3 図は、CRC 生成/送信処理 (2 3 0) の 1 実施例を示すフローチャートである。

CRC 生成/送信処理 (2 3 0) では、Tx-ENC 領域 2 6 2 A から 3 2 ビット単位で暗号化データを読み出して、CRC を生成する。ここでは、暗号化された送信データを対象として説明するが、送信メッセージを暗号化することなく送出する場合は、Tx-BUF 領域 2 6 1 A のデータを CRC の生成対象とすればよい。

まず、Tx-ENC 領域 2 6 2 A から送信メッセージのヘッダ部を読み出し、送信部 1 1 に転送する (2 3 1)。次に、暗号化データの長さ K を 3 2 ビット単位で読み出した場合のデータブロック数 Nmax を計算し、処理の繰り返し回数を示すパラメータ n の値を初期値 “1” に設定する (2 3 2)。

メモリ 5 0 から M-REG 5 1 に CRC 用の行列値 M をロード (2 3 3) した後、Tx-ENC 領域 2 6 2 A から暗号化送信データの最初のデータブロック D(n) を読み出し、送信部 1 1 と B-REG 2 0 3 に転送する (2 3

4)。この状態で積和演算部 40 を起動すると (235)、C-REG 204 に CRC 用行列 M とデータ D(n) との積和演算結果 C0~C31 が出力される。

CRC 生成の場合、積和演算部 40 の一回の起動でデータブロック D(n) に付加すべき CRC 符号が生成できるため、C-REG 204 の内容を送信部 11 に送信し (236)、パラメータ n の値をインクリメントして (237)、n の値を Nmax と比較する (238)。n が Nmax 以下の場合はステップ 234 に戻って、Tx-ENC 領域 262A から次のデータブロック D(n) を読み出し、上述した動作を繰り返し、n > Nmax となった時、1 メッセージ分の CRC 生成処理を終了する。

第 11 図に示した受信データ処理ルーチン 300 における CRC 生成処理 310 は、第 13 図で説明した送信データの CRC 生成ルーチンにおいて、読み出すべきデータブロックの記憶領域を Tx-ENC 領域 262A から Rx-CRC 領域 263B に変更し、ヘッダとデータブロックと CRC の転送先を送信部 11 からバッファメモリの Rx-ENC 領域 262B (平文受信データの場合は Tx-BUF 領域 261B) に変更すればよい。

また、受信データの復号化処理 330 は、Rx-ENC 領域 262B から読み出したデータブロックをメモリ 50 から M-REG 51 にロードした復号化用の部分行列で積和演算処理すればよい。基本的には、第 12 図で説明した送信データ暗号化ルーチンと同様の手順となる。

以上の実施例では行列値演算部 30 で生成した CRC 用、ECC 用の行列をメモリ (MAT-MEM) 50 に格納しておき、CRC 生成と ECC 暗号化/復号化処理を行う時、積和演算部 40 が必要とする行列の値を MAT-MEM 50 から M-REG 51 に適宜ロードするようにしたが、M-REG 51 を CRC 用、ECC 暗号化用、復号化用の専用レジスタとして用意しておき、行列値演算部 30 で生成した行列値をこれらの専用レジ

スタに直接ロードするようにしてもよい。この場合、積和演算部 40 に接続すべき M-REG 51 を切替えることによって、CRC 生成と ECC 暗号化／復号化処理を高速に行うことが可能になる。

また、実施例では、行列値演算部で生成する行列の基本サイズを 3  
5  $2 \times 32$  としたが、これを  $8 \times 8$ 、または  $16 \times 16$  のように小型化した場合、CRC 用の行列も部分行列モードで生成することになる。この場合、CRC 行列値生成ルーチン 100 に、第 10 図で説明した ECC 行列値生成ルーチン 120 と同様の制御手法を採用すればよい。

本発明によれば、予め用意した行列値を利用することによって、送  
10 受信データの誤り検出に必要な CRC 符号を高速に生成できる。また、CRC 用の行列を生成する行列値演算部を利用して、ECC 暗号化用および復号化用の行列値を迅速に生成できる。従って、安全性を高めるために暗号鍵を適宜変更したい場合に、外部から暗号鍵データを与えて、制御部 70 に ECC 行列生成ルーチンを実行させることにより、  
15 暗号鍵に応じた新たな行列値を容易に生成することが可能となる。

#### 産業上の利用可能性

本発明によれば、誤り検出符号生成と暗号化処理にハードウェア（行列値演算部と積和演算部）を共用できるため、コンパクトなパケット  
20 通信装置を提供できる。また、暗号化／復号化処理に必要な行列値をパケット通信装置内で生成できるため、暗号鍵変更が容易であり、送受信データの安全性を向上できる。

## 請 求 の 範 囲

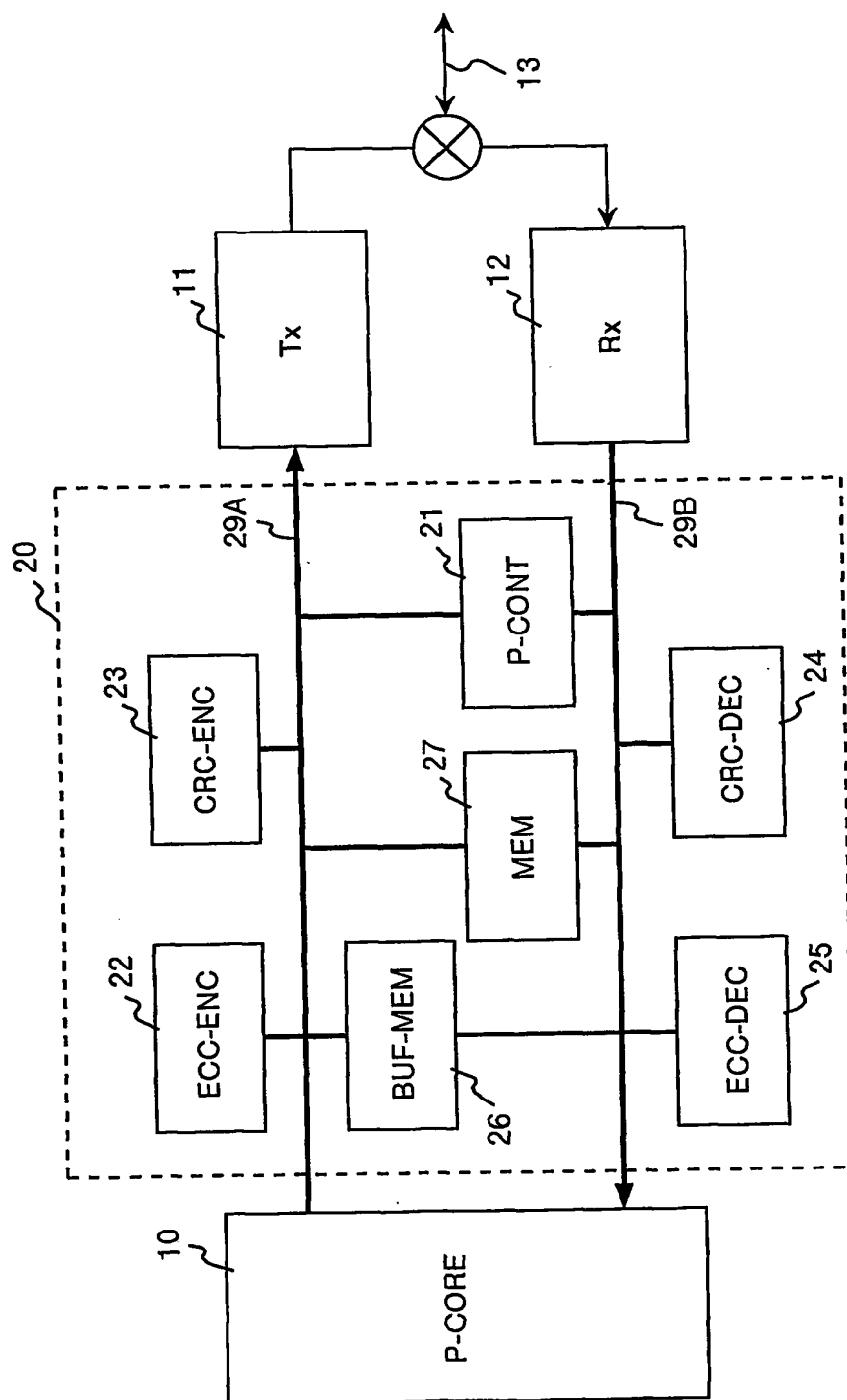
1. それぞれ所定ビット長のパラメータが設定される第1、第2レジスタ(201、202)と、符号化すべきデータが設定される第3レジスタ(203)と、上記第1、第2レジスタの設定値から行列値を生成する行列値演算部(30)と、上記行列値演算部で生成された行列値を保持する行列値レジスタ(51)と、上記行列値レジスタが保持する行列値と上記第3レジスタに設定されたデータとの積和演算を実行する積和演算部(40)とを有し、
- 10 上記第1、第2レジスタの設定パラメータを変えることによって、上記行列値演算部で誤り検出用の行列値と暗号化用の行列値を選択的に生成し、上記行列値レジスタに保持する行列値を切替えることによって、上記積和演算部で誤り符号化演算と暗号化演算を選択的に行うことを特徴とする符号演算装置。
- 15 2. 少なくとも一方に $n$ 次多項式の係数値データが設定される第1、第2レジスタ(201と202)と、符号化すべきデータが設定される第3レジスタ(203)と、上記第1、第2レジスタの設定値から $n \times n$ の行列値を生成する行列値演算部(30)と、上記行列値演算部で生成された行列値を保持する行列値レジスタ(51)と、上記行列値レジスタが保持する行列値と上記第3レジスタに設定されたデータとの積和演算を実行する積和演算部(40)とを有し、
- 20 上記第3レジスタに送信データまたは受信データを供給することによって、上記積和演算部から符号化データを得るようにしたことを特徴とする符号演算装置。
- 25 3. 前記行列値演算部で誤り検出用の行列値を生成し、前記積和演算部から前記第3レジスタの設定データと対応する誤り検出符号を得る

ことを特徴とする請求項 2 に記載の符号演算装置。

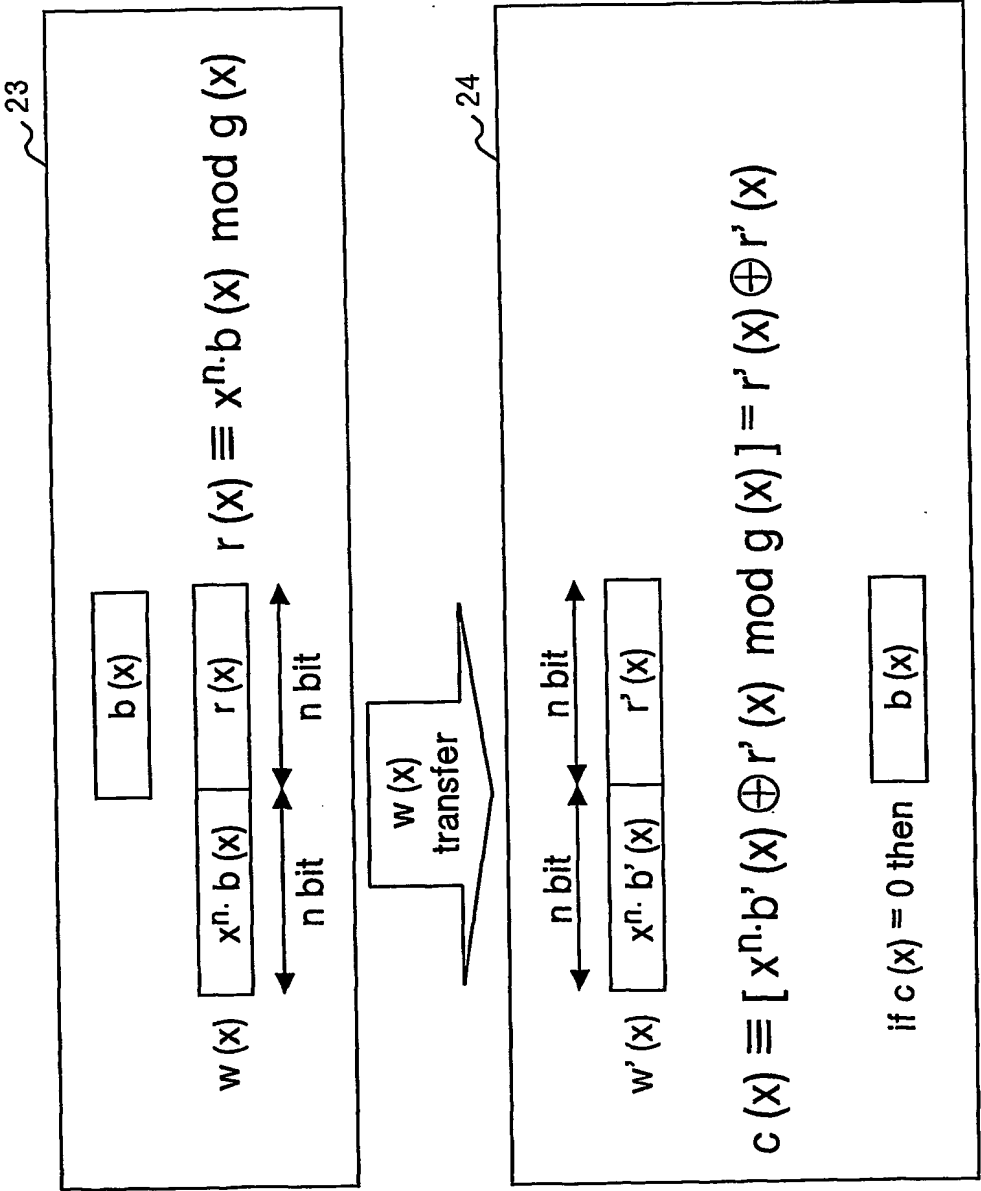
4. 前記第 1、第 2 レジスタに、ガロア体の  $n$  次の多項式  $g(x)$  の最高次  $n$  の係数を除いた係数データ ( $g'$ ) を設定し、前記積和演算部から、前記第 3 レジスタの設定データに対する多項式  $g(x)$  を法 ( $\text{mod}$ ) とする CRC 符号を得ることを特徴とする請求項 3 に記載の符号演算装置。
5. 前記行列値演算部で暗号化用の行列値を生成し、前記積和演算部から前記第 3 レジスタの設定データの暗号化符号を得ることを特徴とする請求項 2 に記載の符号演算装置。
- 10 6. ガロア体の  $n$  次既約多項式  $g(x)$  の係数データと暗号鍵データを記憶するための第 1 メモリと、上記メモリから係数データと暗号鍵データをそれぞれ複数のデータブロックに分割して読み出し、前記第 1、第 2 レジスタに設定する制御部 (70) と、複数の部分行列値を記憶するための第 2 メモリとを備え、
- 15 前記行列値演算部 (30) で  $n \times n$  の複数の部分行列値を生成し、上記制御部の制御の下で、上記行列値演算部で生成された部分行列値を上記第 2 のメモリに記憶しておき、上記第 2 のメモリから前記行列値レジスタ (51) に部分行列値を選択的にロードし、前記積和演算部で前記第 3 レジスタの設定データと複数の部分行列値との積和演算を繰り返すことによって、前記暗号化符号を得ることを特徴とする請求項 5 に記載の符号演算装置。
- 20 7. 前記積和演算部で生成された積和演算結果を中間演算値として保持されている既演算値に排他的論理和加算し、新たな中間演算値として保持するための手段を (52、53) 有することを特徴とする請求項 6 に記載の符号演算装置。
- 25



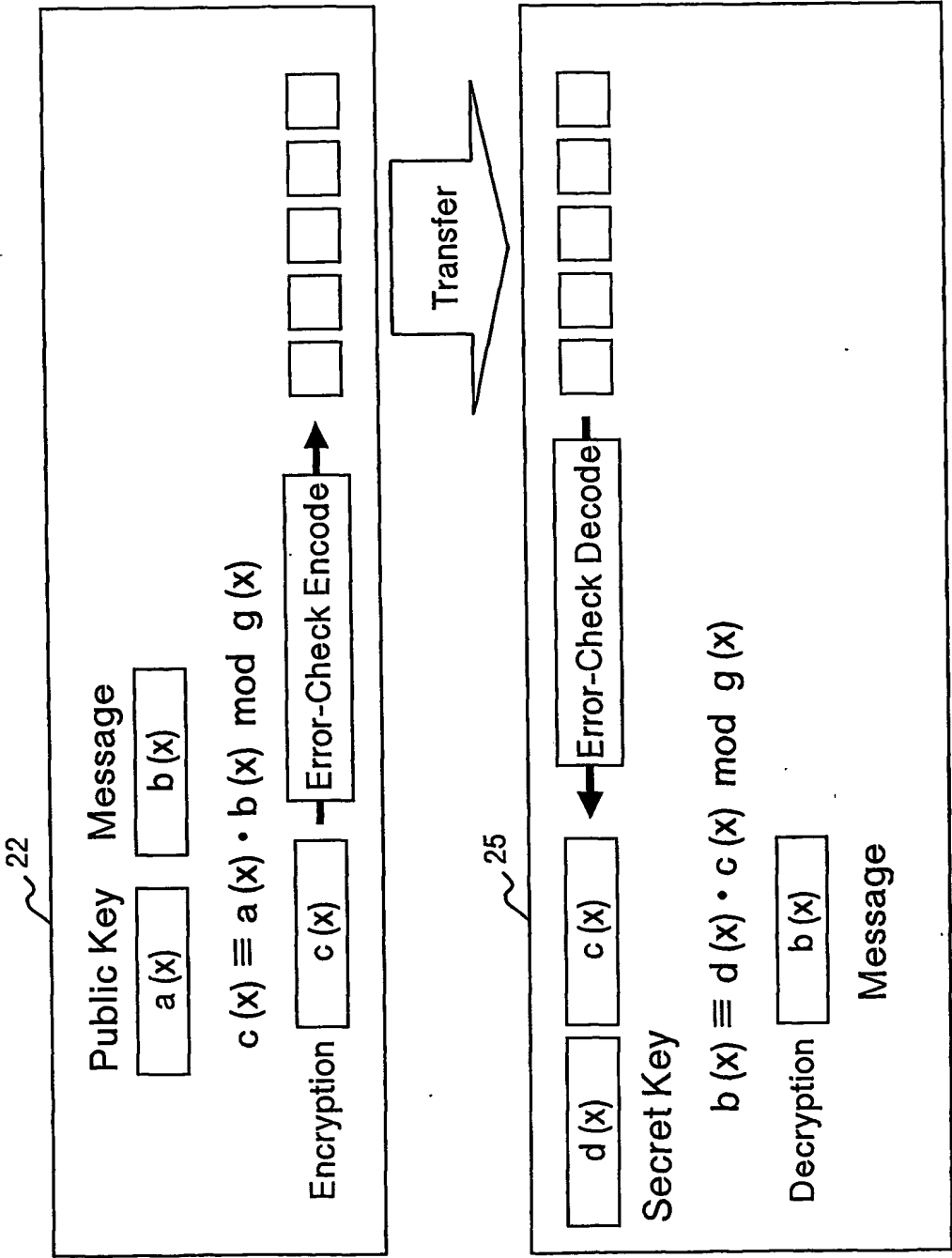
圖一 振



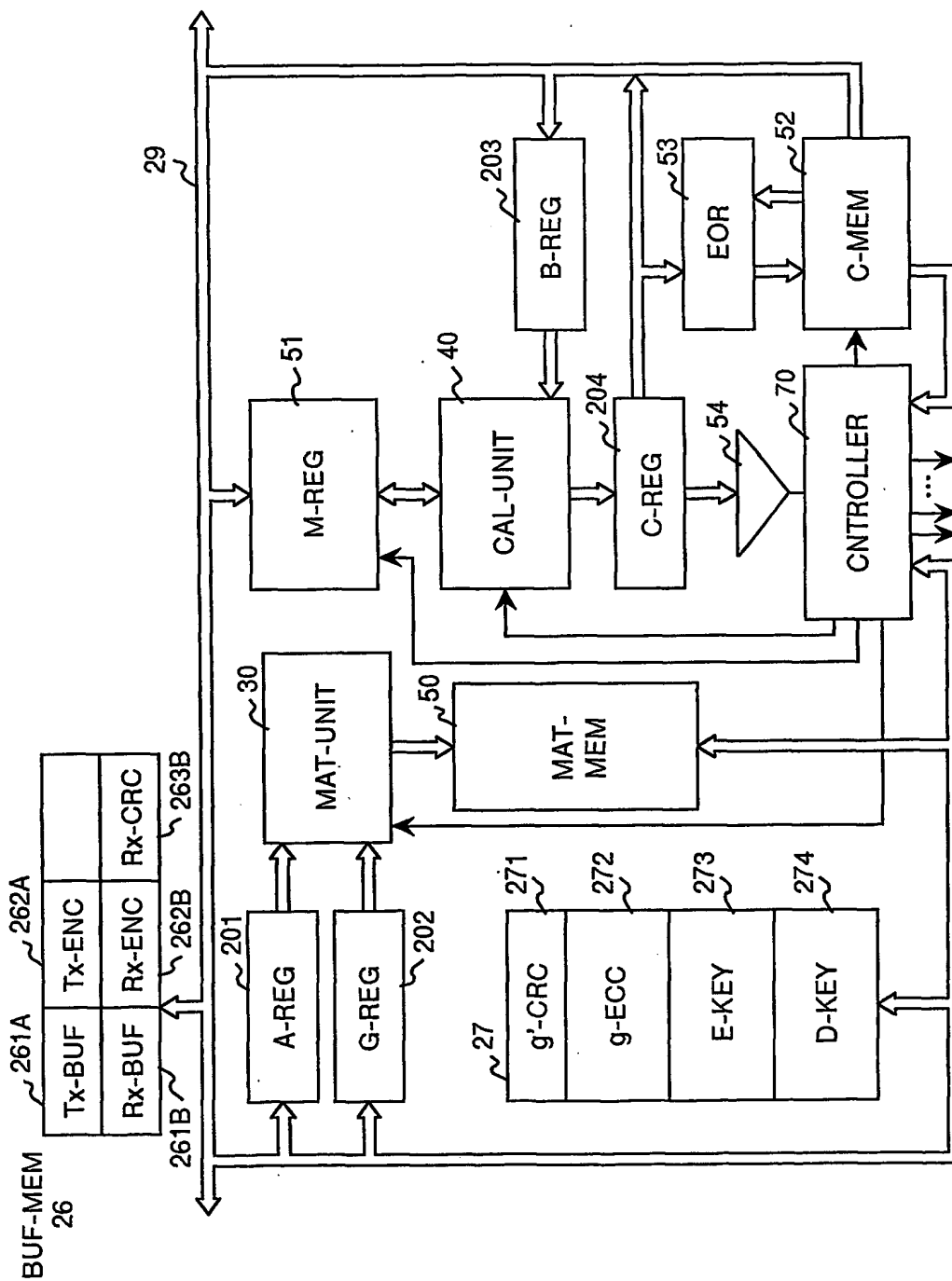
第2図



第3図



第 4 図



5/13

第5図

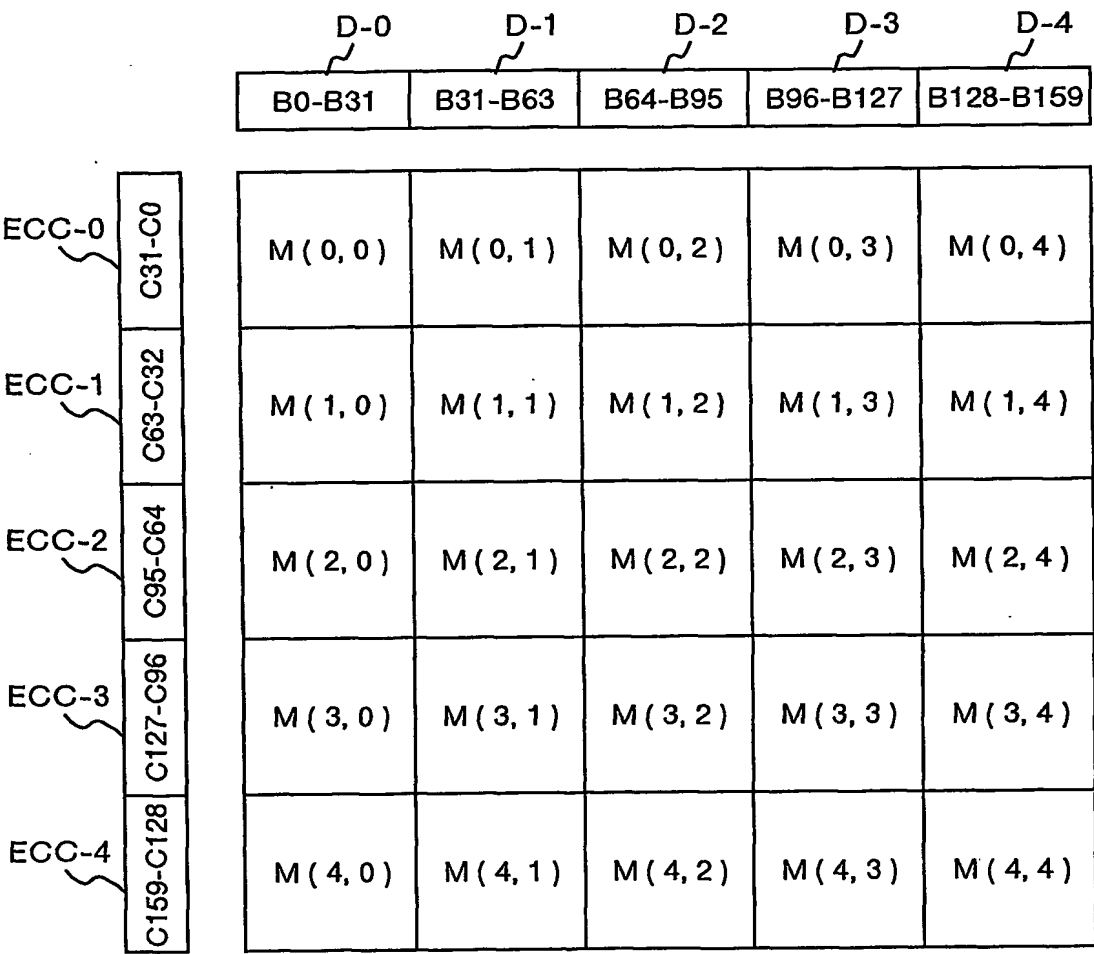
	$b_0$	$b_1$	$b_2$	$b_3$	$b_4$	$b_5$	$b_6$	$b_7$
$c_0$	$m_{00}=a_0$	$m_{01}=g_0m_{70}$	$m_{02}=g_0m_{71}$	$m_{03}=g_0m_{72}$	$m_{04}=g_0m_{73}$	$m_{05}=g_0m_{74}$	$m_{06}=g_0m_{75}$	$m_{07}=g_0m_{76}$
$c_1$	$m_{10}=a_1$	$m_{11}=m_{00}+g_1m_{01}$	$m_{12}=m_{01}+g_1m_{02}$	$m_{13}=m_{02}+g_1m_{03}$	$m_{14}=m_{03}+g_1m_{04}$	$m_{15}=m_{04}+g_1m_{05}$	$m_{16}=m_{05}+g_1m_{06}$	$m_{17}=m_{06}+g_1m_{07}$
$c_2$	$m_{20}=a_2$	$m_{21}=m_{10}+g_2m_{01}$	$m_{22}=m_{11}+g_2m_{02}$	$m_{23}=m_{12}+g_2m_{03}$	$m_{24}=m_{13}+g_2m_{04}$	$m_{25}=m_{14}+g_2m_{05}$	$m_{26}=m_{15}+g_2m_{06}$	$m_{27}=m_{16}+g_2m_{07}$
$c_3$	$m_{30}=a_3$	$m_{31}=m_{20}+g_3m_{01}$	$m_{32}=m_{21}+g_3m_{02}$	$m_{33}=m_{22}+g_3m_{03}$	$m_{34}=m_{23}+g_3m_{04}$	$m_{35}=m_{24}+g_3m_{05}$	$m_{36}=m_{25}+g_3m_{06}$	$m_{37}=m_{26}+g_3m_{07}$
$c_4$	$m_{40}=a_4$	$m_{41}=m_{30}+g_4m_{01}$	$m_{42}=m_{31}+g_4m_{02}$	$m_{43}=m_{32}+g_4m_{03}$	$m_{44}=m_{33}+g_4m_{04}$	$m_{45}=m_{34}+g_4m_{05}$	$m_{46}=m_{35}+g_4m_{06}$	$m_{47}=m_{36}+g_4m_{07}$
$c_5$	$m_{50}=a_5$	$m_{51}=m_{40}+g_5m_{01}$	$m_{52}=m_{41}+g_5m_{02}$	$m_{53}=m_{42}+g_5m_{03}$	$m_{54}=m_{43}+g_5m_{04}$	$m_{55}=m_{44}+g_5m_{05}$	$m_{56}=m_{45}+g_5m_{06}$	$m_{57}=m_{46}+g_5m_{07}$
$c_6$	$m_{60}=a_6$	$m_{61}=m_{50}+g_6m_{01}$	$m_{62}=m_{51}+g_6m_{02}$	$m_{63}=m_{52}+g_6m_{03}$	$m_{64}=m_{53}+g_6m_{04}$	$m_{65}=m_{54}+g_6m_{05}$	$m_{66}=m_{55}+g_6m_{06}$	$m_{67}=m_{56}+g_6m_{07}$
$c_7$	$m_{70}=a_7$	$m_{71}=m_{60}+g_7m_{01}$	$m_{72}=m_{61}+g_7m_{02}$	$m_{73}=m_{62}+g_7m_{03}$	$m_{74}=m_{63}+g_7m_{04}$	$m_{75}=m_{64}+g_7m_{05}$	$m_{76}=m_{65}+g_7m_{06}$	$m_{77}=m_{66}+g_7m_{07}$

第 6 図

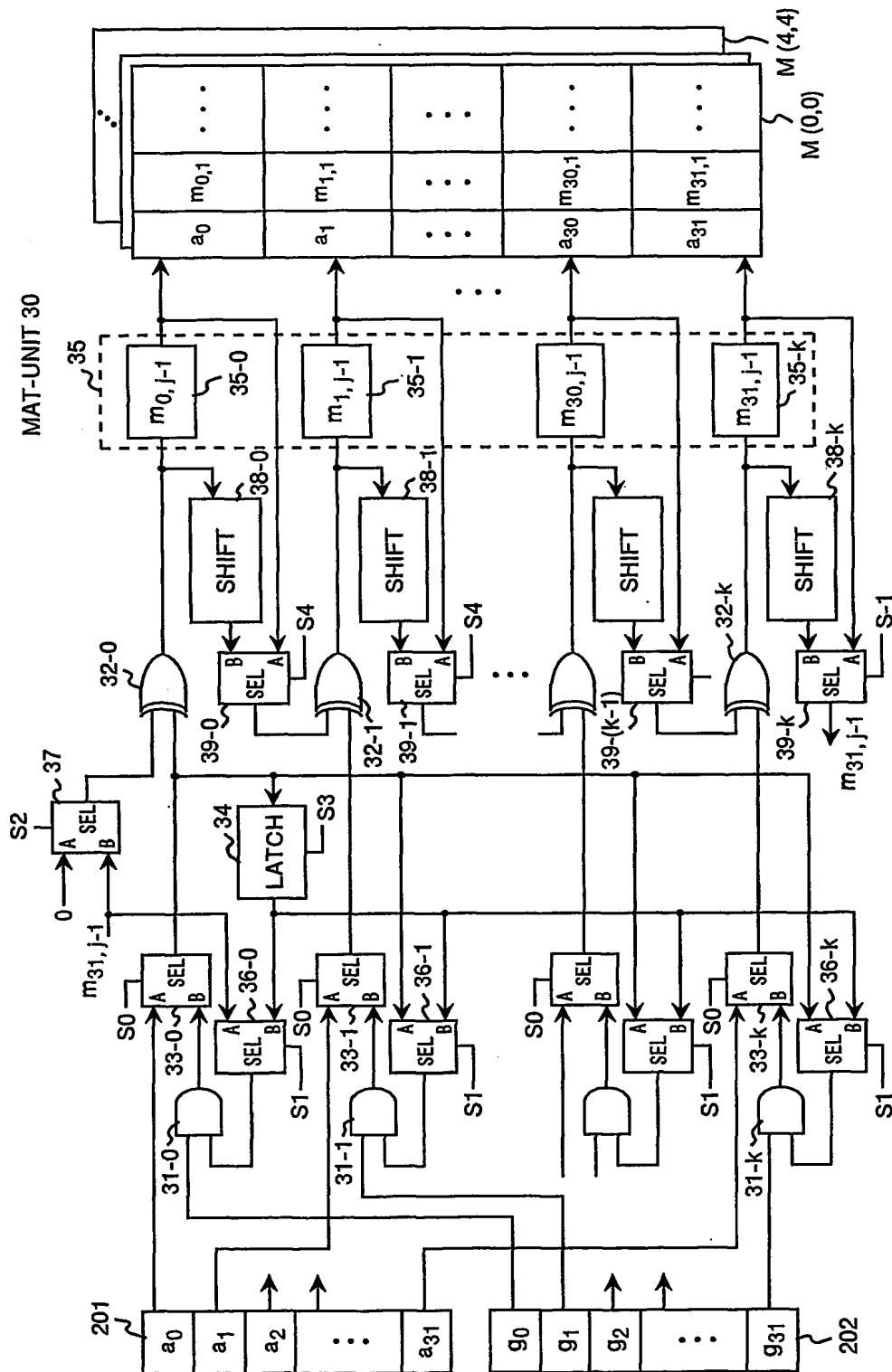
	$b_0$	$b_1$	$b_j$	$b_{j+1}$
$C_0$	$m_{0,0} = a_0$	$m_{0,1} = m_{n-1,0}$	$m_{0,j} = m_{n-1,j-1}$	$m_{0,j+1} = m_{n-1,j}$
$C_1$	$m_{1,0} = a_1$	$m_{1,1} = m_{0,0} + g_1 m_{0,1}$	$m_{1,j} = m_{0,j-1} + g_1 m_{0,j}$	$m_{1,j+1} = m_{0,j} + g_1 m_{0,j+1}$
$C_{n-2}$	$m_{n-2,0} = a_{n-2}$	$m_{n-2,1} = m_{n-3,0} + g_{n-2} m_{0,1}$	$m_{n-2,j} = m_{n-3,j-1} + g_{n-2} m_{0,j}$	$m_{n-2,j+1} = m_{n-3,j} + g_{n-2} m_{0,j+1}$
$C_{n-1}$	$m_{n-1,0} = a_{n-1}$	$m_{n-1,1} = m_{n-2,0} + g_{n-1} m_{0,1}$	$m_{n-1,j} = m_{n-2,j-1} + g_{n-1} m_{0,j}$	$m_{n-1,j+1} = m_{n-2,j} + g_{n-1} m_{0,j+1}$

$M(0,0)$   $M(0,j)$   $M(l,0)$   $M(l,j)$

第 7 図



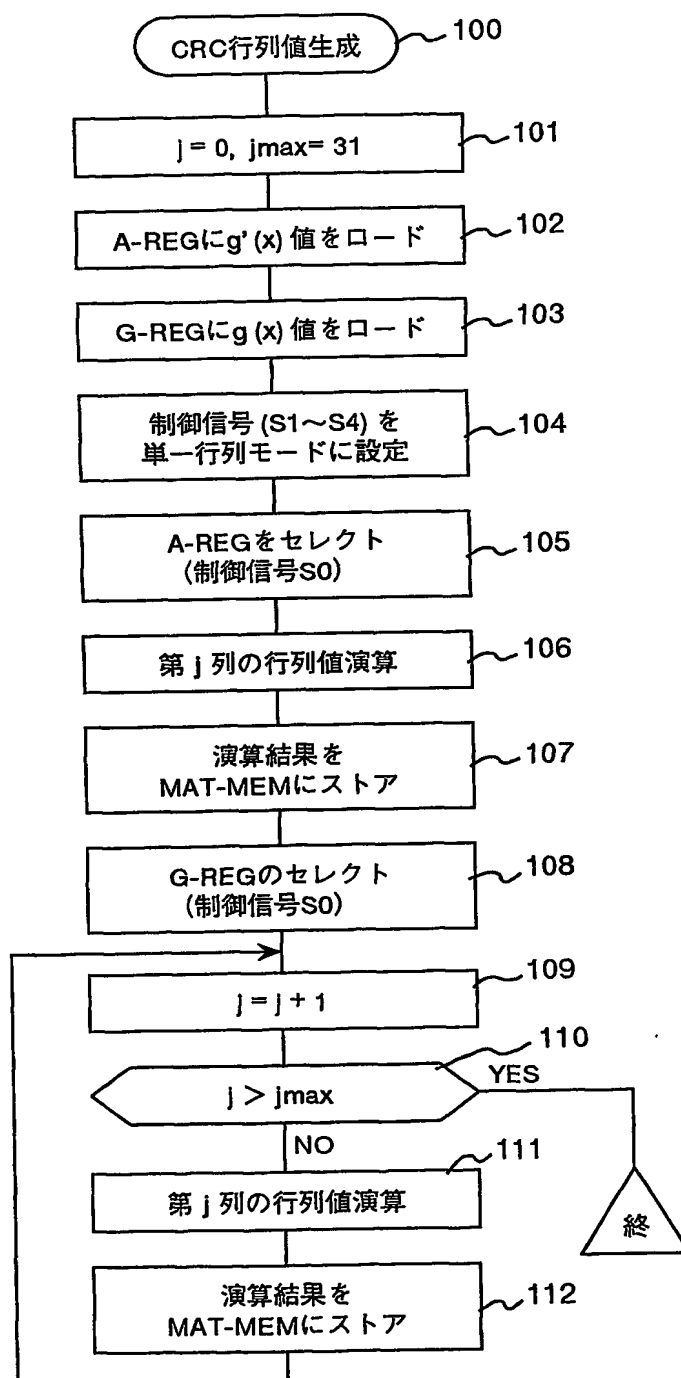
第 8 図





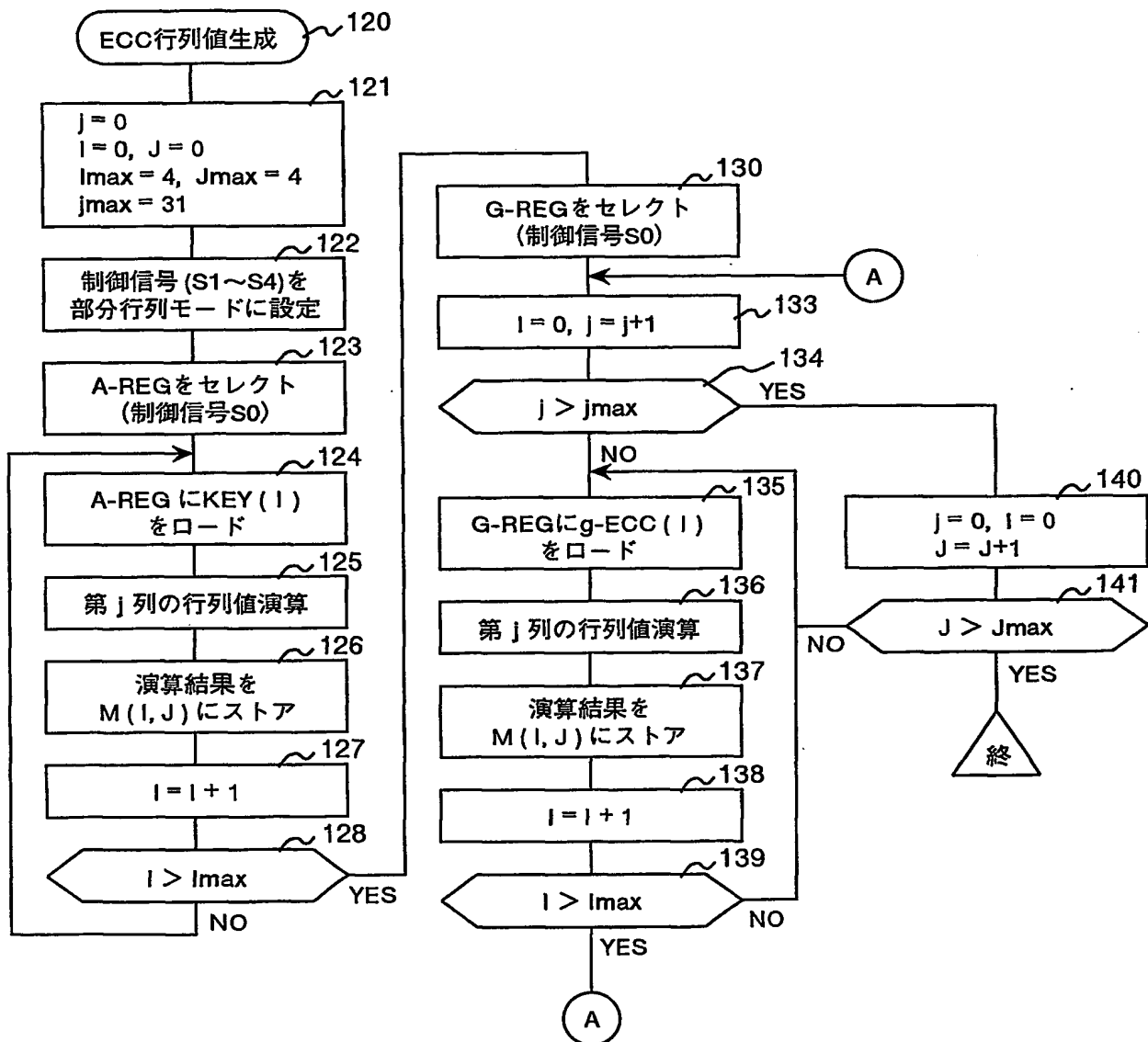
9/13

第 9 図

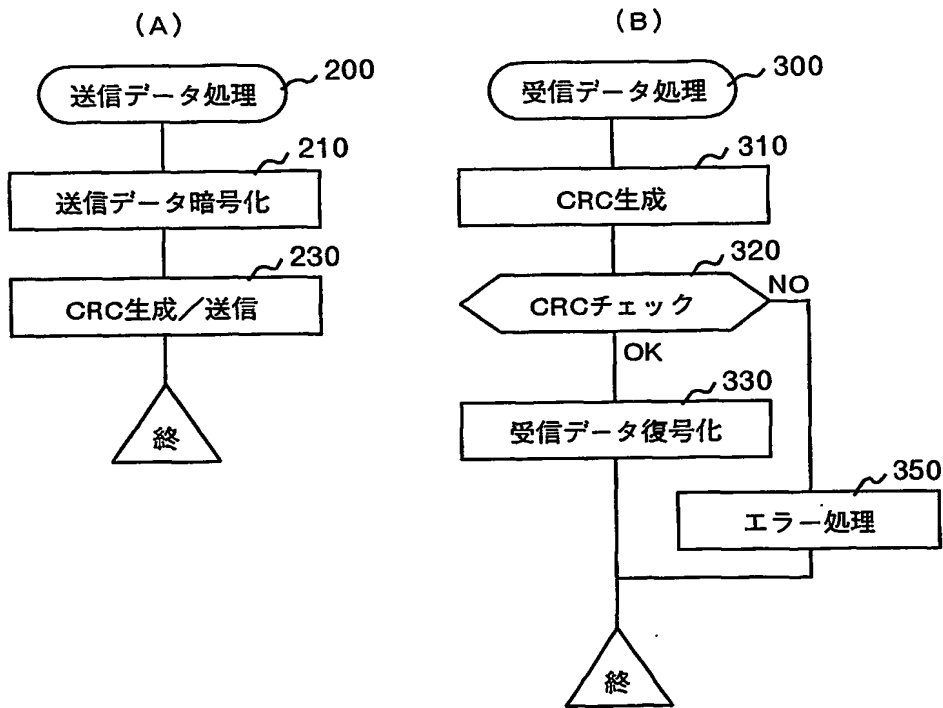


10/13

第 10 図

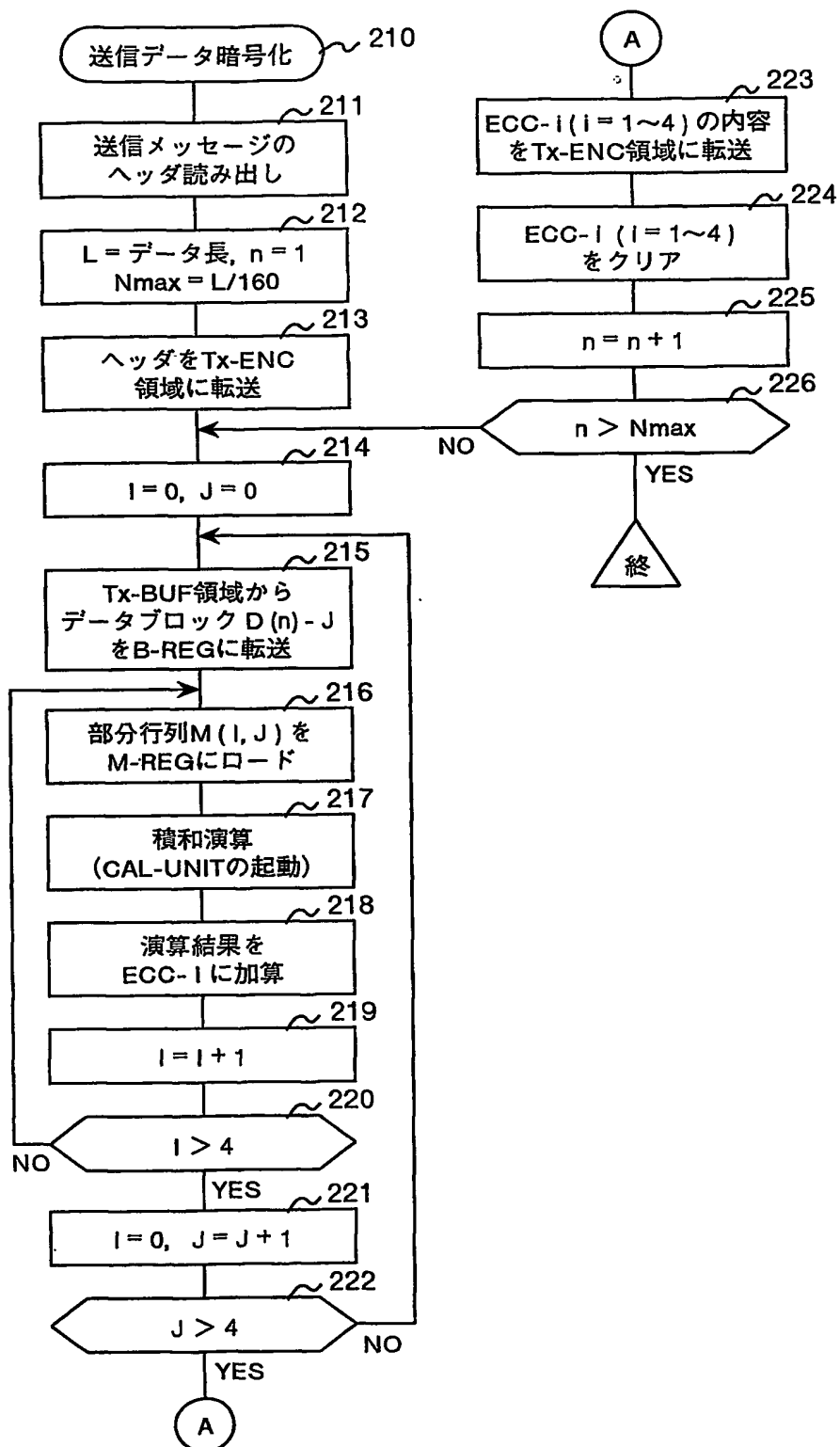


第 1 1 図



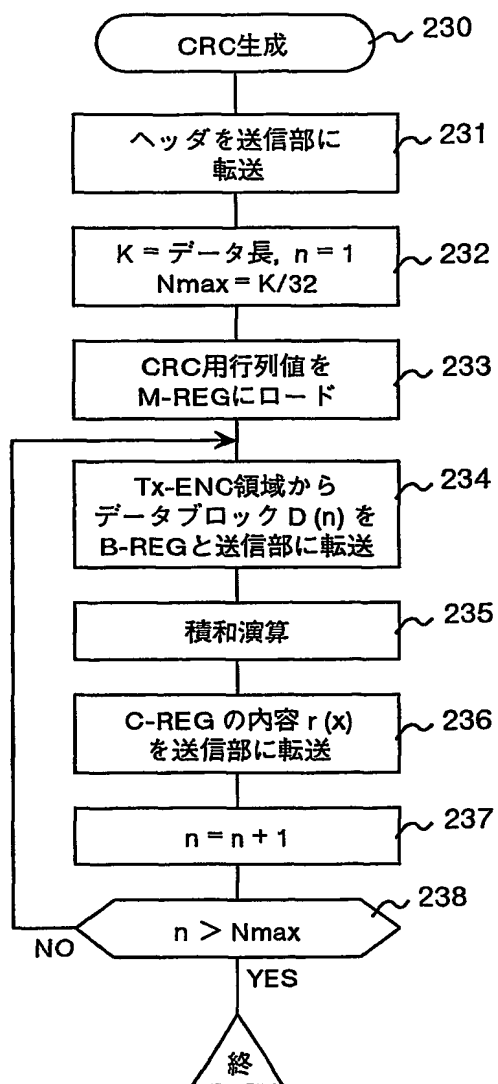
12/13

第 1 2 図



13/13

第 13 図



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/06166

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G09C1/00, H03M13/15, H04L9/30, G06F11/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G09C1/00, H03M13/15, H04L9/30, G06F11/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 91/20028 A1 (MASTROVITO, Edoardo), 31 May, 1991 (31.05.91), Full text; Figs. 1 to 4 & AU 8076591 A & SE 9002124 A	1-7
Y	Kazue SHIBA, Shin'ichi KAWAMURA, Jun SHINBO, "GF(2 <sup>m</sup> ) Ensan oyobi Seisu Ensan o Shori Kano na Hybrid Coprocessor no Teian", 1999nen Ango to Joho Security Symposium Yokoshu, 26 January, 1999 (26.01.99), Volume II of II, pages 819 to 824	1-7
Y	JP 2001-56640 A (Toyo Communication Equipment Co., Ltd.), 27 February, 2001 (27.02.01), Full text; Figs. 1 to 4 (Family: none)	1-7

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
20 September, 2002 (20.09.02)Date of mailing of the international search report  
08 October, 2002 (08.10.02)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/06166

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 7-50595 A (Toshiba Corp.), 21 February, 1995 (21.02.95), Full text; Figs. 1 to 15 & DE 69414631 C & EP 620654 A & US 5517509 A	1-7

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G09C1/00 H03M13/15 H04L9/30 G06F11/10

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G09C1/00 H03M13/15 H04L9/30 G06F11/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年

日本国公開実用新案公報 1971-2002年

日本国登録実用新案公報 1994-2002年

日本国実用新案登録公報 1996-2002年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	WO 91/20028 A1 (MASTROVITO, Edoardo) 1991. 05. 31 全文, FIG. 1-4 & AU 8076591 A & SE 9002124 A	1-7
Y	斯波万恵, 川村信一, 新保淳; "GF (2 <sup>m</sup> ) 演算及び整数演算を 処理可能なハイブリッド・コプロセッサの提案" 1999年暗号と情報セキュリティシンポジウム予稿集, 1999. 01. 26, Volume II of II, p. 819-824	1-7

☒ C欄の続きにも文献が列举されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」同一パテントファミリー文献

国際調査を完了した日

20.09.02

国際調査報告の発送日

08.10.02

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳



5M

4229

電話番号 03-3581-1101 内線 3597



C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P 2001-56640 A (東洋通信機株式会社) 2001.02.27, 全文, 図1-4 (ファミリーなし)	1-7
Y	J P 7-50595 A (株式会社東芝) 1995.02.21 全文, 図1-15 & DE 69414631 C & EP 620654 A & US 5517509 A	1-7